IN THE UNITED STATES DISTRICT COURT 12:00:00
EASTERN DISTRICT OF VIRGINIA 12:00:00
NORFOLK DIVISION 12:00:00

12:00:00
12:00:00
12:00:00

CENTRIPETAL NETWORKS, INC.,) 12:00:00
) 12:00:00
Plaintiff,) 12:00:00
v.) Civil Action No.: 12:00:00
) 2:18cv94 12:00:00
CISCO SYSTEMS, INC.,) 12:00:00
) 12:00:00
Defendant.) 12:00:01

12:00:01
12:00:01
12:00:01
12:00:01
12:00:01
12:00:01

TRANSCRIPT OF VIDEOCONFERENCE BENCH TRIAL PROCEEDINGS 12:00:01

12:00:01
12:00:01
12:00:01

Norfolk, Virginia 12:00:01
June 11, 2020 12:00:01

12:00:01
12:00:01

Volume 22 12:00:01
Pages 3253-3427 12:00:01

12:00:01
12:00:01

BEFORE: THE HONORABLE HENRY C. MORGAN, JR. 12:00:01
United States District Judge 12:00:02

12:00:02
12:00:02

Appearances: (Via Zoomgov Video) 12:00:02

12:00:02

KRAMER LEVIN NAFTALIS & FRANKEL, LLP 12:00:02
By: PAUL ANDRE 12:00:02
JAMES RUSSELL HANNAH 12:00:02
Counsel for Plaintiff 12:00:02

12:00:02

DUANE MORRIS, LLP 12:00:02
By: LOUIS NORWOOD JAMESON 12:00:02
MATTHEW CHRISTOPHER GAUDET 12:00:02

12:00:02

INDEX 12:00:02

12:00:02

12:00:02

	Plaintiff	Defendant	Rebuttal	12:00:03
				12:00:03
Infringement:				12:00:03
				12:00:03
'193	3262	3270	3281	12:00:03
'806	3283	3292	3300	12:00:03
'205	3301	3310	3313	12:00:03
'856	3314	3324	3332	12:00:03
'176	3334	3427	3350	12:00:03
				12:00:04

Validity:	Defendant	Plaintiff	Rebuttal	12:00:04
				12:00:04
'193	3354	3362	3366	12:00:04
'806	3368	3375	3379	12:00:04
'856	3381	3386	3392	12:00:04
'176	3394	3398	3402	12:00:04
				12:00:04

Willfulness:	Plaintiff	Defendant	Rebuttal	12:00:04
				12:00:04
	3406	3411	3414	12:00:04
				12:00:04
				12:00:04

PROCEEDINGS 12:00:04

12:00:04

12:00:04

(Proceedings commenced at 10:02 a.m. as follows:) 12:00:04

12:00:04

COURTROOM DEPUTY CLERK: Civil Action No. 2:18cv94, 10:02:43
Plaintiff, Centripetal Networks, Inc. v. Defendant, Cisco 10:02:47
Systems, Inc. 10:02:47
For the plaintiff, Mr. Andre, Mr. Noona, are you ready 10:02:51
to proceed? 10:02:53

MR. NOONA: Good morning, Your Honor. We are. 10:02:56

COURTROOM DEPUTY CLERK: For the defendants, Mr. Carr, 10:02:59
Mr. Jameson, are you ready to proceed? 10:03:00

MR. JAMESON: Yes, we are. 10:03:02

THE COURT: All right. I've looked at the schedule. 10:03:05
It looks fine to me. So I guess we hear from Centripetal first? 10:03:10

MR. ANDRE: Thank Your Honor. May it please the 10:03:17
Court. Paul Andre. I hope we stick to the schedule. We'll do 10:03:19
our best. 10:03:22
First of all, I'd like to start off with thanking Your 10:03:24
Honor. This has been a great, an interesting privilege trying 10:03:26
the very first Zoom case in federal court. We appreciate Your 10:03:30
Honor's patience with us. 10:03:34
I also want to thank the court staff. Lori, Brandon, 10:03:36
Carol, Paul and everyone behind scenes for making this as 10:03:38
seamless as possible. It has been a truly unique experience, 10:03:43

and I know how much hard work this takes to do it right. 10:03:45

We started this case, Your Honor, talking about 10:03:49
Centripetal. And I put a timeline up. And you'll see the slide 10:03:53
as we go through them. And this is a company that literally 10:03:56
when they were formed in 2009 in the basement of Steven Rogers' 10:04:00
house, they wanted to change the world. They wanted to change 10:04:05
the way things were done. They wanted to create a new market. 10:04:07
And they believed they could. Mr. Rogers had had 40-plus years 10:04:10
of secure communication under his belt. He saw a problem that 10:04:15
he thought he could uniquely solve with the people he knew. And 10:04:19
in this case we've brought our top executives. We brought 10:04:27
Mr. Rogers, the president, CEO and founder. We brought Dr. Sean 10:04:31
Moore, the chief technology officer and chief scientist. We 10:04:36
brought Jonathan Rogers, the chief operating officer, and Chris 10:04:39
Gibbs, the vide-president of global sales. We brought our 10:04:42
executives here to tell Centripetal's story. Notably absent 10:04:45
from Cisco was any of their executives. They brought engineers, 10:04:51
but no executives. And that speaks volumes. We'll talk about 10:04:54
that later. 10:04:57

The story that we told about Centripetal was a company 10:04:59
that started off with a new idea. They worked very hard at 10:05:01
their ideas, many times without pay. They raised a lot of money 10:05:08
to fund their new ideas. And they protected their ideas. They 10:05:12
filed patents. The five patents in this case are a result of 10:05:16
those filings. They put the time and effort in, and they do 10:05:24

what young startup companies are supposed to do. They protected their IP. 10:05:28 10:05:32

What they didn't know was that there was a press release that would change their world. You saw this exhibit many times. PTX-452. On June 20th, 2017, says "Cisco unveils a network -- one of the most significant breakthroughs in enterprise networking. They didn't realize in June of 2017 how this press release was going to change their world. It took them five months to learn that what Cisco had done was take the technology that Centripetal provided to them and used it in their own products. What they didn't realize when this press release came out in June 20th, 2017 was nearly eight and a half to nine years of work was going to be put in jeopardy. Because when you have the biggest company in the word, biggest networking company in the world using your technology, it's nearly impossible to compete. So it was eight and a half to nine years worth of work, tens of millions of dollars that they raised to fund that work, was in jeopardy. 10:05:35 10:05:40 10:05:45 10:05:54 10:05:59 10:06:03 10:06:07 10:06:11 10:06:16 10:06:21 10:06:25 10:06:29 10:06:32 10:06:35 10:06:39 10:06:42

We gave you a timeline to show you how Cisco and Centripetal had interactions starting in June of 2015 all way till the end of 2016, December of 2016. For a year and a half Centripetal thought they had a potential partner with Cisco. They were looking for investment. They were looking for a co-partnership with them, presenting their own products, and they believed them. In '15 they gave all public confidential -- 10:06:48 10:06:54 10:07:01 10:07:06 10:07:08 10:07:12 10:07:15

I mean non-confidential information. In January 2016, six 10:07:19
months after meeting with Cisco, Cisco wanted to sign a 10:07:23
non-disclosure agreement to get more information, and from 10:07:27
January 2016 to December 2016, Centripetal, under the belief 10:07:30
that they were being protect under the non-disclosure agreement, 10:07:36
they gave them everything. They told them about their 10:07:39
algorithms, they told them about their patents, they told them 10:07:41
about their technology, they demonstrated it numerous times. 10:07:44
Cisco kept coming back and asking for more. And they provided 10:07:47
it to them. It wasn't until six months after they had their 10:07:50
last meeting that Cisco launched the Network Intuitive. 10:07:53

Now in this case, to prove our infringement, we 10:07:58
provided the Court with a lot of exhibits. Maybe too many at 10:08:02
times. But we kind of serve two masters here with the Federal 10:08:04
Circuit and the District Court. We're always concerned that we 10:08:08
don't give enough evidence, the Federal Circuit would not like 10:08:10
it. But we did give a lot of proof, and we're going to go 10:08:13
through those today. The key exhibits. Not all of them, 10:08:17
obviously. The key exhibits we're going to go through today. 10:08:19

But what I want to focus on now before we start 10:08:22
turning to infringement is how Cisco responded to those claims 10:08:25
of infringement. They had a non-infringement formula. They 10:08:29
first said Cisco did not provide security. That's incredible. 10:08:33
I want to talk about that. They mischaracterized our expert's 10:08:40
testimony, they rewrote the claim language, they used they 10:08:44

cartoon diagrams, never their own technical documents, to show 10:08:47
how the systems worked, and they ignored their technical 10:08:51
documents. What I want to talk about very quick, then I'm going 10:08:55
to turn it over it Mr. Hannah to talk about the '193 patent. 10:08:58
The first point is they denied their product provides security, 10:09:01
which was an credible statement. We showed you the SEC filing 10:09:05
in which Cisco talked about, they announced that they were 10:09:09
presenting a brand-new technology, network-based technology from 10:09:12
a security standpoint. The Catalyst 9000 switches represented 10:09:16
the initial build of intent-based networking. Security was 10:09:20
foundational. And in the SEC filing, you look at that last 10:09:23
sentence, "We intend to protect and provide security against the 10:09:29
entire tech continuum, before, during and after a cyber attack." 10:09:32
Before, during and after. 10:09:37

They come to this court and said they don't do it 10:09:39
before, they don't do it during, they only do it after. But 10:09:41
they told the SEC, the public, the world, they did it before, 10:09:46
during and after that cyber attack. 10:09:49

They also launched a brand-new operating system. The 10:09:53
IOS was a -- built from the ground up. And you see at the top, 10:09:58
"Built for security. At Cisco, security is our top priority." 10:10:01
And yet, they built a brand-new operating system from the ground 10:10:04
up, focused on security, and they said it did not provide 10:10:08
security. 10:10:12

We showed you PTX-1287 where they talk about the 10:10:12

Catalyst 9000 switches. They detect and stop threats, once 10:10:18
again, going with the before, during and after time period 10:10:22
again. But they come to this court saying they don't do it 10:10:26
before, they don't do it during, they don't do it after. 10:10:30

We showed you PTX-199. This is Catalyst At A Glance 10:10:33
where it talks about end-to-end security. "Detect and stop 10:10:37
threats, even with encrypted traffic. Putting security above 10:10:40
everything helps putting security above everything helps you 10:10:44
innovate while keeping your assets safe." 10:10:50

We showed you Exhibit PTX-1260. Once, against built 10:10:53
for security, Catalyst switches. Says it detects and stops 10:10:59
threats. End-to-end security integrated. 10:11:02

We looked at the StealthWatch, Exhibit 482. 10:11:05
StealthWatch talks about detect and respond to threats in 10:11:10
real-time. There's a big debate about what is real-time. 10:11:14
Shouldn't be any debate at all. Everyone knows what real-time 10:11:18
is. They denied what real-time was. Real-time is real-time. 10:11:22
When it's not real-time, they say near real-time. 10:11:25

Going to PTX-992 talks about StealthWatch being able 10:11:30
to detect advanced threats before we can turn into a breach. 10:11:34

Finally, turning to the benefits of StealthWatch, 10:11:38
"Real-time detection after attacks by immediately detecting 10:11:41
malicious connections." Immediately connecting. They deny what 10:11:47
the word immediately means. They talked about proactive 10:11:51
protection as well in Exhibit PTX-962. 10:11:54

Now their formula for invalidity involved Cisco used 10:11:58
old stuff. I said that in my opening statement. And you look 10:12:02
at what they used, they used what I call the Name Game. My 10:12:06
favorite name game I use at these kind of trials is the Ford 10:12:09
Mustang. You look at a '65 Ford Mustang and a 2020 Ford 10:12:12
Mustang, they're both Mustangs, but they're very different cars. 10:12:17
You may like a '65 better. I prefer to have a '65. But they're 10:12:20
different cars altogether. But they're both called Ford 10:12:24
Mustang, but they're very, very different. What Cisco did was 10:12:28
say the old StealthWatch and new StealthWatch, the same thing. 10:12:30
Old Catalyst, new Catalyst, same thing. They had brand names, 10:12:34
but that was it. 10:12:37

Finally I want to turn to whether or not saying to the 10:12:38
public about this new network, chuck Robbins, their CEO, we'll 10:12:40
talk about this, this is Exhibit 1890. Talked about how they 10:12:44
had to -- the most significant achievement in 10 years. They 10:12:47
had to rewrite 25 years of source code and had to rewrite the 10:12:51
entire operating system. They talked about Encrypted Traffic 10:12:55
Analytics being one of the most revolutionary innovations that 10:12:57
are out there. 10:13:02

And finally, before I turn it over to Mr. Hannah, they 10:13:02
also talked about Cisco launched a new era in networking in 10:13:05
PTX-451 saying that the Catalyst switching portfolio constitute 10:13:08
mobile cloud performance integrated security. We're releasing 10:13:13
something no one in the market can do, which is basically the 10:13:18

ability to understand whether there is malicious traffic in 10:13:22
encrypted traffic without decrypting it. 10:13:26

So Your Honor, I'm going to turn it over to Mr. 10:13:28
Hannah. I know we're on a clock here, but this is what we'll be 10:13:31
looking at when we look at these. So I'll roll out of the way 10:13:33
and let Mr. Hannah take it over. 10:13:37

MR. HANNAH: First off, I just want to thank Your 10:13:53
Honor, thank also the court staff, thank everyone who's helped 10:13:56
participate in this trial and made it come to fruition. It has 10:13:59
been a pleasure, and we do appreciate it. 10:14:02

If it may please the Court, may I proceed? 10:14:05

THE COURT: You may. 10:14:08

MR. HANNAH: Thank you, Your Honor. So I'll be 10:14:08
talking about the '193 patent. The '193 patent is what we've 10:14:10
characterized as the forward or drop patent. And echoing Mr. 10:14:17
Andre's statements, this is a way to keep your assets safe. You 10:14:21
keep your assets safe by being able to program the switches and 10:14:25
routers to prevent malicious traffic and malicious actors from 10:14:29
exfiltrating your data from the network. And that's what we 10:14:34
talked about during this trial again and again. The '193 10:14:39
prevents data transfers to protected resources, but it allows 10:14:44
date transfers to unprotected resources. And the reason is 10:14:47
simple: You want to protect those resources, these servers that 10:14:51
have your credit card information, that have your personal 10:14:56
information from being accessed, but at the same time, you don't 10:14:58

want to hinder productivity. You want to allow a user to be 10:15:02
able to do their work on the daily basis, but you still want to 10:15:08
protect those protected resources. And that's what the '193 10:15:13
patent is about. 10:15:15

We showed you Dr. Mitzenmacher and we showed you a 10:15:18
number of exhibits. 10:15:21

THE COURT: All right. What was the filing date on 10:15:22
this patent? 10:15:27

MR. HANNAH: It is on -- the filing date is 10:15:28
March 12th, 2013. That's the priority date, Your Honor. 10:15:31

THE COURT: Right. Okay. Go ahead. 10:15:36

MR. HANNAH: So Dr. Mitzenmacher was our expert who 10:15:40
testified regarding the '193 patent, and he showed you a number 10:15:43
of exhibits that are listed here on the screen. He was also the 10:15:46
one that identified Cisco's infringing switches. As Your Honor 10:15:50
knows, this is the Catalyst 9000 platform and included the 9300, 10:15:54
the 9400 and the 9500. 10:15:59

We also discussed the infringing routers. This was 10:16:02
the Aggregated Services Router, the Integrated Services Router, 10:16:05
and the Series 4000 Integrated Services Router. All of these 10:16:10
switches and routers, they have one thing in common. Well, 10:16:16
multiple things in common, but one thing in particular for 10:16:19
infringement: They all include the same operating system. And 10:16:23
that's 16.5 and later versions of the IOS. And based on that 10:16:25
operating system, they contain a number of functionality, 10:16:30

including this quarantine functionality. 10:16:34

And so when we look at Dr. Mitzenmacher's opinion, his 10:16:38 opinion was that these 9000 switches, the routers, the ASR 10:16:43 routers, the ISR routers, they infringe the '193 patent. And 10:16:50 it's just the switches and routers. One of the points that 10:16:55 comes out from this case was trying to confuse this issue, but 10:16:57 it's just the switches and routers and it's the functionality 10:17:01 that they include on those switches and routers. And what they 10:17:03 do is they have packet filtering rules and they perform a number 10:17:08 of different things in a number of different stages and steps. 10:17:12 So first they apply what are these SGT tags. We had discussion 10:17:15 about this. They call them Scalable Group Tags, they call them 10:17:21 Secure Group Tags. There's no dispute they operate in the same 10:17:26 manner: That you apply these tags to the packets. 10:17:29

THE COURT: All right. They apply the tags when the 10:17:33 packets enter the network? 10:17:39

MR. HANNAH: When the packets are going from -- they 10:17:42 can be applied when they come into the network, but also when a 10:17:46 user on the network has been quarantined, these tags will be 10:17:49 applied to all of the traffic that is leaving from that user. 10:17:55 So this is how the user is able to access -- not access 10:18:02 protected resources, but be able to access things like the 10:18:07 Internet. 10:18:11

THE COURT: Why do they put the tags on? 10:18:13

MR. HANNAH: They put the tags on in order to identify 10:18:15

the user as being quarantined. So when I -- 10:18:17

THE COURT: Who is the user? 10:18:26

MR. HANNAH: The user could be an employee in a 10:18:27
corporation. 10:18:29

THE COURT: All right. So are they tagged on -- as I 10:18:31
recall, when it enters, but the tag doesn't automatically cause 10:18:35
it to quarantine. 10:18:43

MR. HANNAH: That's correct, Your Honor. That's 10:18:44
correct. 10:18:47

THE COURT: In other words, it goes through another 10:18:47
switch or router after the tag is put on it? 10:18:49

MR. HANNAH: That's exactly correct, Your Honor. 10:18:56

THE COURT: And it's at that point that the decision 10:18:57
is made whether or not to quarantine the packet? 10:19:00

MR. HANNAH: That's exactly correct, Your Honor. 10:19:05
Exactly correct. You attach those tags, another switch or 10:19:07
router will look at that tag. Based on that tag it will 10:19:11
determine and apply a quarantine policy. That's what we're 10:19:14
talking about in the second bullet point. Looking at that tag, 10:19:17
it applies this quarantine policy. Based on that policy, the 10:19:21
switch or the router is going to make a decision. It's going to 10:19:25
either prevent the data transfer from going to a protected 10:19:30
resource, and it does that by applying these operators that are 10:19:36
discussed in the claims. This is the deny bridge or the deny 10:19:40
route that Dr. Mitzenmacher talks about. That's one option. 10:19:42

The second option is based on, if the packet is destined for an 10:19:47
unprotected resource such as the Internet or something else that 10:19:53
is not your credit card database, it will apply a second 10:19:58
operator which says, okay, I'm going allow this packet to go 10:20:01
forward. And that's the analysis that the switches and the 10:20:05
routers do. 10:20:10

So we looked at a number of -- a lot of evidence with 10:20:14
the switches and routers. And if we go to the next slide we see 10:20:18
that this is fundamentally built into the switches. This is 10:20:21
PTX-126 talking about this security is built into the switches. 10:20:26

We go to the routers. If we look at the routers on 10:20:31
the next slide, this is PTX-1226, talking about how this 10:20:33
security is built into the routing solutions. 10:20:38

Looking at 1262, which is on next slide, this is some 10:20:42
of the evidence showing these are the Scalable Group Tags. This 10:20:46
is how those tags are applied and analyzed. This is from the 10:20:50
switches from PTX-1262. 10:20:53

We go to PTX-1280. It talks about how the SGT 10:20:57
assignment is changed which creates the quarantine based on the 10:21:02
tag we just discussed, Your Honor. And then these fabric edge 10:21:06
devices, the switches and the routers, those apply the 10:21:11
quarantine policy that we just discussed to allow whether we're 10:21:13
going to have network access or not. 10:21:17

This is summed up in a diagram in which it shows how 10:21:19
the quarantine procedures works. So you have the supplier or 10:21:24

your employee. This diagram uses the supplier. And it determines, okay, we need to quarantine the supplier because it looks like there might be some malicious activity going on. 10:21:29 10:21:36 10:21:38

So if you go to the next slide, you apply the quarantine policy at the switch. And as you can see, all of the protected resources are in red. And so your first operator, your deny bridge, deny route, will deny that supplier from going to any of those. However, if that supplier is trying to go to the Internet, trying to do their work, trying to do whatever they wanted to do, it's allowed to the Internet. And that's the second operator. The second operator says this is going to the Internet, that data transfer is okay, I'm going to allow it. 10:21:42 10:21:45 10:21:49 10:21:54 10:21:59 10:22:03 10:22:07 10:22:10 10:22:13

THE COURT: When do they put the tags on? 10:22:17

MR. HANNAH: As you said, they put the tags as soon as the -- 10:22:19 10:22:21

THE COURT: Where in this diagram do they put the tags on? 10:22:22 10:22:25

MR. HANNAH: It's not really shown in this diagram. And that is going to be within where the quarantine circle is, within that. It will be the first switch -- like you said, Your Honor, the first switch that the supplier goes to through that traffic gets the tag applied. And then a subsequent switch or a subsequent router will look at that tag and apply the quarantine. That's exactly what Your Honor, the scenario that Your Honor said. This is just showing that you have the, some 10:22:26 10:22:28 10:22:31 10:22:36 10:22:39 10:22:42 10:22:46 10:22:50

data transfers that are prevented and other data transfers that 10:22:53
are allowed. That's what this is showing. 10:22:56

THE COURT: All right. 10:23:00

MR. HANNAH: Your Honor, so if we look at the claims, 10:23:00
and we look at what all of these claims that -- we walked 10:23:03
through each of these claims. You receive the packets, you 10:23:06
apply these packet filtering rules to event a particular type of 10:23:10
data transfer, that's important, to prevent the data transfer, 10:23:13
you apply the operator, and you drop the packet. And then if 10:23:17
it's allowed, it's responsive that it doesn't correspond to that 10:23:20
criteria, then you apply the second operator which forwards the 10:23:24
packet. That's what these claims require and that's exactly 10:23:27
what this functionality does. 10:23:31

When we look at the non-infringement case, the only 10:23:32
element that was challenged was the one or more packet filtering 10:23:36
rules configured to prevent a particular type of data transfer 10:23:40
from a first to a second network. What happened was on 10:23:43
cross-examination they actually admitted that this element was 10:23:48
present. I took the -- or crossed Dr. Crovella. And during his 10:23:51
cross, I was very specific and I was very clear. I asked "Let's 10:23:59
on the quarantine rules. Now, the quarantine rules, those are 10:24:06
packet filtering rules, correct?" 10:24:09

"Yes, they are." 10:24:12

He admitted that they're packet filtering rules. Then 10:24:13
I asked him a second question right away. I said "Now, those 10:24:16

quarantine rules, they are capable of preventing data transfer, 10:24:20
correct?" 10:24:23

"Certainly, yes." 10:24:26

When you look at the claim, if you look at the claim 10:24:27
language and you look at what they're trying to contest, 10:24:30
Dr. Crovella on cross-examination admitted that that element is 10:24:34
present. 10:24:38

So what did they do for non-infringement? They 10:24:41
rewrote the claims. Instead of saying that you have packet 10:24:45
filtering rules that are configured to prevent a data transfer, 10:24:50
which Dr. Crovella admitted that they had, they rewrote the 10:24:53
claims and came up with a non-infringement position saying that 10:24:57
you have to inspect the payload of the packet. That's not what 10:25:02
the claim says. That's a complete rewriting of the claim. 10:25:06
Claim says that you prevent a particular type of data transfer, 10:25:11
and all of the evidence that we've shown, including the 10:25:14
cross-examination of their witness, proves that all these 10:25:17
elements are met. 10:25:20

If Your Honor has any questions, I'm happy to answer 10:25:23
those, otherwise we can pass it to the other side. 10:25:27

THE COURT: All right. I'll hear from the other side. 10:25:32

MR. JAMESON: Good morning, Your Honor. Woody 10:25:42
Jameson. May I proceed? 10:25:43

THE COURT: You may. 10:25:46

MR. JAMESON: Thank Your Honor. It's been a long 10:25:46

trial, and we're all ready to be done. I want to echo the 10:25:48
comments from Mr. Andre. Thanks to you for persevering through 10:25:53
all this with us, and thanks to your staff. They have been 10:25:57
amazing in helping us get through this process. 10:26:01

I want to -- I was actually shocked by what Mr. Andre 10:26:05
said, that Cisco's denied that we provide security. I 10:26:10
literally -- I don't even know what he's talking about. I mean, 10:26:15
we began this case in my opening statement putting up books that 10:26:18
are thousands of pages long talking about Cisco providing 10:26:22
network security going back to 1999. Books that we provide to 10:26:26
the industry to teach them about network security. Courses that 10:26:32
actually Dr. Cole, their expert, has taken as part of him 10:26:35
learning how to be an expert in this case and in the industry. 10:26:38
Cisco is proud of the network security that it provides. It 10:26:44
just doesn't infringe these patents. 10:26:50

And the observation that we didn't bring our 10:26:54
high-ranking executives to this case, Your Honor, this is a 10:26:58
patent case. We're dealing with technical issues, and we 10:27:04
brought the most sophisticated, knowledgable technical 10:27:07
subject-matter experts from Cisco to testify about the 10:27:12
technology that's at issue in this case. Hari Shankar, Peter 10:27:17
Jones, David McGrew, Michael Scheck, Danny Llewallyn. These are 10:27:22
the people that actually developed the products that are being 10:27:26
accused of infringement. That's exactly what you're supposed to 10:27:30
do in this case. 10:27:35

With that, Your Honor, this is our opportunity to put 10:27:39
the pieces of the puzzle together. I know at times during this 10:27:43
trial there's been occasions where things didn't seem to fit or 10:27:47
things didn't seem to be relevant. But we now have a complete 10:27:52
record. And what we're going to do today is we're going to show 10:27:55
why we don't infringe these patents. Mr. Gaudet and I, we 10:27:59
believe in the strength of our case. With every bit of 10:28:03
conviction, we know we don't infringe these patents. And at 10:28:07
times, the search for the truth through their subject-matter 10:28:12
experts or their technical experts has caused frustration. Has 10:28:15
caused confusion. I will never, ever hear the word 10:28:21
"obfuscation" again without a mental image of Your Honor. I 10:28:25
think that would be true of the experts and all the lawyers in 10:28:30
this case. But the confusion and the frustration at times has 10:28:35
been because there is a cavernous gap between what the claim 10:28:41
language actually covers and what they are accusing of 10:28:46
infringement. And the gap at times is so big that things just 10:28:51
don't make sense. And we are going to pull that together for 10:28:57
you today. 10:29:01

But before I turn it over to Mr. Gaudet, I want to 10:29:03
start with the bedrock principle of patent law and patent 10:29:08
infringement, and that is that Centripetal has the burden to 10:29:14
show that every limitation of every claim is met. And as these 10:29:17
cases state, the failure to meet a single limitation is 10:29:23
sufficient to negate infringement of the claim. And I put this 10:29:28

up here because, Your Honor, the words of these claims matter. 10:29:31
The steps and the ordering of the claims matter. The antecedent 10:29:39
basis issues in referencing back up to earlier elements in the 10:29:44
claims, it all matters when you try to show infringement. And 10:29:48
when you focus on the words -- and that's, you know, the name of 10:29:55
the game is the claim, and the words in the claim, they can't 10:29:58
show infringement. 10:30:02

The other legal issue -- and we've been, quite frankly 10:30:05
the parties have been back and forth about this now for the 10:30:09
better part of however long we've been going. Non-infringement 10:30:11
and invalidity can be argued in the alternative. And we have 10:30:15
made reference to 01 Communique a number of times, but I wanted 10:30:19
to put up some language from the case, because it's really 10:30:24
important. And in that case, and this is a quote, "Citrix also 10:30:27
presented an alternative invalidity defense that focused on its 10:30:32
prior art BuddyHelp product. It argued that under the trial 10:30:36
court's claim construction, claims 24 and 45 were valid, but not 10:30:42
infringed, but that if Communique attempted to expand the scope 10:30:47
of its claims to include the accused system, then the claims 10:30:52
would be invalid in light of the prior art." And the Federal 10:30:57
Circuit held. "There was nothing improper about this argument." 10:31:01

And that is what our experts have done. They have 10:31:07
explained why we don't infringe, but when they have turned to 10:31:11
invalidity, they have accepted as correct Centripetal's 10:31:16
infringement contentions and explained why the patents would be 10:31:21

invalid under the infringement contentions. 10:31:26

The final point from this case. "As we have 10:31:29
previously recognized, when an accused product and prior art are 10:31:34
closely aligned, it takes exceptional linguistic dexterity to 10:31:37
simultaneously establish infringement and evade liability." 10:31:45

That's what we have here. And Centripetal does not 10:31:50
have the exceptional linguistic dexterity to walk that tight 10:31:54
rope. 10:32:00

And Your Honor, a final point on the law and then I'm 10:32:01
going to turn it over to Mr. Gaudet. And we already heard it in 10:32:03
the opening: What matters here is the technical operations of 10:32:06
the product. It's not about marketing materials. And we cite 10:32:10
to you a number of cases that say just that. "Marketing 10:32:15
materials are insufficient evidence of infringement when 10:32:21
unsupported by evidence of the actual operation of the product." 10:32:23
I've never seen so many marketing materials in my life in a 10:32:27
patent case. We want to focus on the technical documents. And 10:32:30
what we should be looking at in this kind of case we should be 10:32:34
looking at source code. We should be looking at technical 10:32:39
specifications. Maybe we should look at white papers and data 10:32:42
sheets. But the least-relevant evidence is marketing materials, 10:32:45
and that is what they have built their case on. 10:32:50

And with that, I am going to turn it over to Mr. 10:32:54
Gaudet to talk about the '193 patent. 10:32:56

MR. GAUDET: Thank you. And good morning, Your Honor. 10:33:11

I am jumping forward to slide 14 in your binder. Let me start 10:33:14
by also thanking the Court and the Court staff -- 10:33:20

THE COURT: What binder is this we're talking about? 10:33:23

MR. GAUDET: Your Honor, you should have a Cisco 10:33:26
closing binder that's got our presentation in it. 10:33:29

THE COURT: Okay. 10:33:45

MR. GAUDET: And we'll actually jump -- this is now 10:33:46
the '193 patent. We'll jump all the way to Slide 16, Your 10:33:48
Honor. 10:33:51

Your Honor, I listened to Mr. Hannah's closing very 10:34:05
carefully, and it actually sounds to me like it would be what we 10:34:09
fundamentally have here is a dispute about the claim scope; that 10:34:11
in their view, this patent broadly covers dropping or allowing 10:34:16
packets. And that's just not what the patent's about. And if 10:34:20
it was, it would have died in the IPR. But they told the Patent 10:34:24
Office something very specific to save the patent. What this 10:34:29
patent's about specifically is a particular type of rules that 10:34:32
stop exfiltration. And I've got here some language from the 10:34:36
background, it's the specification, that points to the fact that 10:34:40
these aren't just any old drop or allow rules, these are 10:34:43
specific rules to stop exfiltrations. 10:34:46

Now, why does that matter? Okay. We agree, all we're 10:34:50
talking about here are the quarantine rules. Are quarantine 10:34:53
rules, do they satisfy this one or more packet filtering rules 10:34:56
configured to prevent a particular type of data transfer from 10:35:02

the first network to the second network. That's the dispute. 10:35:06
And what this comes down to, Your Honor, is what that claim 10:35:09
language means. 10:35:13

Your Honor, as our expert, the specification, the 10:35:15
claim language, their statements to the Patent Office and one of 10:35:22
their experts all confirmed, this claim requires what everyone 10:35:26
refers to as a two-stage. And Your Honor, the first stage, the 10:35:30
first stage we've highlighted the claim language here in green. 10:35:39
That's the question, where is the packet going? What's the 10:35:43
destination? Where did it come from, where is it going? And 10:35:46
Your Honor, quarantine rules do that. That is what the 10:35:49
quarantine rules do. But that's all the quarantine rules do. 10:35:51
They say where did it come from, if it came from a quarantined 10:35:54
user, where is it going, and it drops it for almost all 10:35:59
destinations and it will allow it for certain others. But 10:36:02
that's it. That is the first stage of the rule that is the 10:36:05
first stage of the filtering process. That's all they do. 10:36:09

That's not what this patent covers. To get this 10:36:14
patent and to keep it valid, there is a second stage. And that 10:36:17
second stage, Your Honor, is where we win this patent. It's 10:36:22
where we win this case. The second stage requires that you look 10:36:25
to see what particular type of data transfer it is. And that's 10:36:29
where the rubber hits the road in terms of exfiltrations. 10:36:34
Particular types of data transfers indicate exfiltrations. So 10:36:38
it's not that block all packets to a given destination. It's 10:36:43

that you only block these packets to the given destination that 10:36:50
have the particular type of data transfer. That's in the claim 10:36:53
language, but it's in a lot of other places, Your Honor. 10:36:57

The next place I will go is the specification. This 10:36:59
language in the specification, it refers to the claims as having 10:37:06
a two-stage process. Says the first stage uses this 5-Tuple 10:37:10
that's in the header and it determines if the network policy 10:37:16
allows any communications between the resources. That's the 10:37:19
destination stuff. The language in red is the second stage. 10:37:22
It's when the application packet field headers are -- when the 10:37:27
second -- I'm sorry. The second highlight here, the second 10:37:35
stage determines if the policy allows the specific method or 10:37:38
type of communication; e.g., file read, file write, encrypted 10:37:42
communications between the resources. 10:37:47

Now Your Honor, I realize this is in the 10:37:49
specification. It matches up with the claim language. But you 10:37:51
may say, well, is that enough? Is that enough to be sure? This 10:37:55
is the nail in the coffin, Your Honor. When we filed, when 10:37:59
Cisco filed an IPR on this patent on this very claim, 10:38:03
Centripetal told the Patent Office this claim requires a 10:38:07
two-stage process. And what I have highlighted here is -- this 10:38:11
is, these are their words, this is their response to the IPR 10:38:16
petition -- they're quoting exactly the same language from the 10:38:19
specification I just showed you. It's the same patent from the 10:38:23
same passage. And they say, "In the second stage you have to 10:38:28

determine if it allows the specific method." They go on, Your 10:38:31
Honor. They said it three times to the Patent Office. This is 10:38:35
now the same document, DTX-369 at Bates 18. And the red one is 10:38:39
the relevant one. "Second. And responsive to that 10:38:44
determination, the computing system applies an operator 10:38:49
configured to drop packets associated with the particular type 10:38:52
of data transfer." And up at the top where they again refer to 10:38:55
this as this two-stage process. 10:38:58

Your Honor, they did it a third time. This is now 10:39:04
DTX -- Page 21, the same document. "The '193 patent introduced 10:39:10
the concept of applying an operator that can determine whether 10:39:14
the packet is associated with a particular type of data 10:39:17
transfer." 10:39:20

So you may ask, why does this matter? Why does it 10:39:22
matter that they said something in an IPR? How does that count? 10:39:25
And Your Honor, the Federal Circuit has definitively answered 10:39:29
that question. It's the top cite here on slide 23, Aylus 10:39:32
Network v. Apple. The Federal Circuit said that Patentee, here, 10:39:38
Centripetal, their statements and their preliminary response to 10:39:42
an IPR petition, which is exactly what we just looked at, they 10:39:46
have the same binding effect as any other prosecution history 10:39:49
statement. It's as if they said that same thing in the original 10:39:54
prosecution to get the claims allowed. And the second quote 10:39:58
here really says it all, that "Extending the prosecution 10:40:02
disclaimer doctrine to IPR proceedings will ensure that claims 10:40:05

are not argued one way to maintain their patentability," namely, 10:40:09
two stages, you've got to have, look for the specific type of 10:40:15
data transfer, "and in a different way against accused 10:40:19
infringers" when suddenly all that matters is the first stage. 10:40:23
And the Federal Circuit held it applies to your statements even 10:40:28
statements in the preliminary response, it doesn't matter if the 10:40:31
Patent Office agreed or not, they're binding. 10:40:36

But there's more, Your Honor. Dr. Orso confirmed 10:40:39
this. Dr. Orso, their invalidity expert, I cross-examined him 10:40:41
on it. This is now slide 24. "You agree it requires these two 10:40:45
stages?" And I have the last question here, "No. 2," reading 10:40:49
from his report, "using an operator to determine whether the 10:40:54
rules allow for the particular type of data transfer. That's 10:40:57
the second stage?" He agreed. 10:41:01

So Your Honor, at this point let's, now that we 10:41:04
understand you've got to have these two stages, it's not good 10:41:08
enough just to look at what the destination packet or origin, 10:41:11
you have to figure out what type of data transfer it is. How do 10:41:18
we apply that here in the accused products? Well, I do think 10:41:21
Mr. Hannah agrees with me that the only thing that's accused 10:41:24
here are these quarantine rules. Slide 25. We had this up 10:41:26
before during the course of trial, but this is Dr. Mitzenmacher 10:41:30
acknowledging that the only thing he accused were the quarantine 10:41:32
rules. So this patent rises or falls on whether or not 10:41:36
quarantine rules perform this second state of that; namely, if 10:41:41

after and in addition to looking at a destination and a source, 10:41:46
do quarantine rules look at the particular type of data transfer 10:41:49
such that some things going to that address are okay, other 10:41:53
things are not. And there is no dispute. They absolutely do 10:41:58
not do that. There can be no dispute. 10:42:01

This document, Your Honor, is a document Dr. 10:42:03
Mitzenmacher relied on. The packet comes in to a router, if 10:42:05
it's got this tag on it, apply input SGACL, that looks at this 10:42:11
tag. If the tag is from -- if the tag has, if it's there, it 10:42:19
knows that it can go to certain destinations, it can't go to 10:42:24
other destinations. That's the end of it. 10:42:28

And Your Honor, to summarize how the quarantine works, 10:42:30
and we've got all the evidence at the bottom here, a quarantine 10:42:36
treats all packets from a quarantined computer the same way 10:42:40
based only on the destination, all right? So a packet from a 10:42:45
quarantined computer, it might be the most innocuous, safe thing 10:42:49
in the world, it still gets blocked. It might be the deadliest 10:42:53
thing in the world, it gets blocked. It's irrelevant what's in 10:42:57
the packet. Quarantining is based only on the packet's address. 10:43:00
And Your Honor, the witnesses agreed on this. You know, 10:43:08
Dr. Crovella, I asked him, "Let's get to the punch line. Is a 10:43:11
quarantine a two-stage rule process?" He said No. I mean, it 10:43:15
"only looks at" -- the green portion of the slide was the 10:43:18
header" where the packet's coming from and where it's going. It 10:43:23
does not ask whether the packet is part of a particular type of 10:43:25

data transfer." 10:43:29
And Your Honor, I want to pull up -- I ask the 10:43:30
plaintiff, if you would, pull up the slide that plaintiff put 10:43:33
up, slide 33. Because they quoted some testimony from Dr. Orso 10:43:37
and I want to be real clear about -- not Dr. Orso, from 10:43:41
Dr. Crovella, and I want to take a look at that. 10:43:46
This is what Mr. Hannah cited as literally the only 10:43:50
evidence that a quarantine rule could do this second step. What 10:43:52
type of data transfer. Look at the question Dr. Crovella was 10:43:57
asked. "The quarantine rules, they are capable of preventing 10:44:01
data transfer." Of course. They block everything. Of course 10:44:06
they prevent data transfer. They don't prevent a particular 10:44:09
type of data transfer. If you apply the first stage and you 10:44:14
block everything to a particular destination, by definition you 10:44:19
have blocked, you have prevented a data transfer in a very 10:44:24
overarching way. That is not what this patent requires. The 10:44:27
patent requires that you block a particular type of data 10:44:32
transfer. And nobody in this case has ever suggested that a 10:44:38
quarantine can figure out if something is a particular type of 10:44:42
data transfer. 10:44:47
Let's go back to our slides. 10:44:51
THE COURT: You're already over time, so let's wind 10:44:55
this up. 10:45:00
MR. GAUDET: Thank you, Your Honor. 10:45:01
THE COURT: They haven't done their rebuttal yet. 10:45:02

MR. GAUDET: I was simply going to make the point, Your Honor, that Dr. Mitzenmacher agreed -- this is now slide 29 -- he agreed that quarantines are simply based on the source and the destination. 10:45:04 10:45:05 10:45:09 10:45:13

And Your Honor, we have a second non-infringement position, but the truth is, this is the one, this is the one that I think we should win this patent on. With that, I'll sit down. 10:45:14 10:45:17 10:45:21 10:45:26

THE COURT: All right. 10:45:28

MR. HANNAH: Thank Your Honor. May I proceed? 10:45:34

THE COURT: You may. 10:45:36

MR. HANNAH: Thank you. 10:45:36

So Your Honor, as anticipated, there's a lot of talk about changing the claim language, and so I want to go back to what the claim language says. If we go to slide 31 of our slides, which is claim 18, this is the actual claim language. And it does not say that you have a packet filtering rule that's configured to inspect for a particular type of data transfer or to inspect the payload. It says it's configured to prevent a particular type of data transfer. And I think one of the points that has to be made crystal clear is that every time that Dr. Orso, the IPRs or anyone else that is reading this patent as it's written and when they talk about the two-stage process, they're talking about the first stage is the packet filtering rule that's configured to prevent -- prevent, that's a key 10:45:37 10:45:41 10:45:44 10:45:48 10:45:56 10:46:00 10:46:04 10:46:09 10:46:13 10:46:17 10:46:25 10:46:29 10:46:34

word -- the particular type of data transfer, the second stage 10:46:37
is applying the operator. 10:46:41

I want to go to, if I can see Dr. Orso's testimony 10:46:44
that counsel just showed you, it's on slide 24 from opposing 10:46:48
counsel. 10:46:52

Counsel showed you this testimony and quickly got off 10:47:01
of it and saying that Dr. Orso agreed that you have to inspect 10:47:03
the payload or do some type of thing. Look at what his answer 10:47:10
actually is. His answer does not agree with the question. He 10:47:13
says the application of the operator is the second stage. And 10:47:18
of course it is. Because that's what the patent requires. When 10:47:22
you look at the record and you look at the IPRs, that's exactly 10:47:25
what the IPRs say. The patent was allowed or institution didn't 10:47:29
get granted because Cisco failed to prove that an operator was 10:47:34
applied. That's the second stage they were talking about. 10:47:38

Now I want to look, they spent a lot of time looking 10:47:42
at the specification. Let me show you figure 3 of the '193 10:47:46
patent which is JTX-4. This is from the specification, and it 10:47:50
shows what these operators can be. Again, counsel's trying to 10:48:06
manipulate the claim language, but when you look at what the 10:48:11
operators can be, there's a column right there, and it says it 10:48:15
can be allow or a block operator. And that's exactly what these 10:48:19
quarantine rules do. You look at the packet filtering, you 10:48:23
apply the packet filtering rules, and if it's going to a 10:48:27
protected resource, you apply the block operator. 10:48:30

With that, Your Honor, I have no more argument unless you have any questions. 10:48:35 10:48:39

THE COURT: No. 10:48:41

MR. HANNAH: Thank you, Your Honor. 10:48:42

THE COURT: Let's move on to the next -- 10:48:46

MR. ANDRE: Your Honor, I get the privilege of doing the '806 patent. This is the rule swapping patent. You preprocess rule sets and you process packets in accordance with the rule sets and the second rule set. The patent has a priority date of January 11th, 2013. 10:48:49 10:48:50 10:48:57 10:49:01 10:49:04

Dr. Mitzenmacher was our expert on this patent. Once again, he provided overwhelming evidence of infringement. There are two product sets that we're going to be talking about, switches and router plus the DNA Center and then the firewalls plus the DNA -- plus the Firepower Management Center, and we'll have to break these up into two different product offerings. 10:49:09 10:49:12 10:49:16 10:49:19 10:49:23 10:49:27

So the switches and routers with the DNA Center, Digital Network Architecture center, if you look at how it's set up and you'll see this is a common theme over these next two patents. You have a management center, in this case it's the DNA Center, and it ingests threat intelligence. And it, threat intelligence, it then sends things down to the routers and switches. When we get to the firewalls you'll see the Firepower Management Center does the same thing, it sends it down to the firewalls. It's just a management center to manage dynamic 10:49:32 10:49:38 10:49:41 10:49:45 10:49:48 10:49:54 10:49:56 10:49:58 10:50:01

security policies or in this case rule swapping. It creates the rules based on the ingestion of threat intelligence. 10:50:06 10:50:10

Now, Dr. Mitzenmacher's opinion on the switches and routers is that the Catalyst 9000 switches, the routers in combination with the DNA infringe '806 patent. The DNA Center ingests rules from a variety of cyber threat intelligence sources, preprocesses the rules to create optimized policies which are distributed to their switches and routers. When the new rules are available and sent to the switches and routers, the switches and routers will perform a rule swap without dropping packets. And that's going to be a key thing. That was the big innovation. How are you going to swap these rules out and not drop packets? It's a very important aspect of this patent. 10:50:14 10:50:16 10:50:21 10:50:25 10:50:27 10:50:33 10:50:36 10:50:39 10:50:42 10:50:44 10:50:47 10:50:51

We showed you a white paper, DTX-1263, that talks about how the DNA Center operates within the routers and switches, how information is in constant flowing back and forth. You see that the DNA Center is learning, it's ingesting this threat intelligence, and ingests this intelligence and when the rules are ready it sends it down where the routers and switches can do the swapping. 10:50:51 10:50:57 10:51:02 10:51:05 10:51:09 10:51:13 10:51:15

What we saw in this case, and this is a technical specification, Exhibit 1195, this is the Hitless ACL. This is the new feature that changes -- does the rule swapping without dropping. So no packets should drop. If you look it what the 10:51:20 10:51:24 10:51:29 10:51:35

problem defined, this is a 2017 document, Exhibit 1195, the problem was that packets were being dropped when they were doing the previous rule swapping. And we'll see that when get to validity where they're overlapping the rules and packets were dealing dropped. With the Hitless ACL Change Flow, the key here was packets would not be dropped. And there is a algorithm, you can see it, an 11-step algorithm that is defined on how these rules are swapped. Now, the evidence that we got in this case, Dr. Mitzenmacher showed you a lot of technical documents. Probably some of the best evidence we got is from Mr. Peter Jones, the witness for Cisco. This was in his deposition. " 10:51:39 10:51:45 10:51:48 10:51:51 10:51:55 10:51:58 10:52:01 10:52:05 10:52:12 10:52:15 10:52:18

What do you mean by Hitless?" This is Hitless ACL. So he's talking about changing from rule set A to rule set B and not drop packets in the middle or have them subject to the rules. So what he's saying is you don't -- you're going to have those packets coming in and at some stage between the two packets is where it would get updated. So that's what he was talking about. 10:52:24 10:52:28 10:52:32 10:52:35 10:52:39 10:52:41 10:52:45

Now so at trial, Mr. Jones came in to testify and talk about this Hitless ACL, and on this next slide it's very difficult to read, it's in your binder, slide 43, and we're also going to put it in as an exhibit to the proposed findings of fact. Next slide. 10:52:46 10:52:50 10:52:55 10:52:58 10:53:01

THE COURT: Just a second. 10:53:05

MR. ANDRE: It's very difficult to read. 10:53:13

THE COURT: Slide 43. 10:53:15

MR. ANDRE: Slide 43 in our binder. That's correct, 10:53:16
Your Honor. 10:53:18

THE COURT: Wait a minute. Let me find it. 10:53:20

MR. ANDRE: Sure. 10:53:22

THE COURT: Okay. 10:53:34

MR. ANDRE: So Mr. Hannah, this is Mr. Hannah's entire 10:53:35
cross-examination of Mr. Jones. I put the whole thing in 10:53:38
without edits. I just put it on the right-hand column. This 10:53:41
was it from start to finish other than the pleasantries of good 10:53:44
afternoon. And Mr. Hannah went through this testimony and just 10:53:47
basically read the claim language, claim 9, into this testimony. 10:53:55
Every single element is met here. You can just look at 10:53:59
Mr. Jones' testimony and he admitted each one of the claim 10:54:03
elements. You combine that with Dr. Mitzenmacher and the 10:54:07
preponderance of the evidence is there. It's much more than 10:54:09
preponderance of the evidence. 10:54:12

"When you talk about receiving a first rule set and a 10:54:14
second rule set," Mr. Hannah asked him, "the Catalyst switches, 10:54:16
do they receive rule sets," plural. "That's correct". And that 10:54:20
comes from the DNA Center. That's where the rule set comes 10:54:22
from. He says that's correct. And then we're talking about 10:54:26
preprocessing and configuring the processors and getting all the 10:54:28
preprocessing step down. How the Catalyst processes these rules 10:54:32
in order to process the rules, in order to process these rules, 10:54:37

the Catalyst switch must compile them right in order to 10:54:41
implement the results? That's correct. In doing the compiling, 10:54:44
it compiles these rules while the old rules are still processing 10:54:48
packets. So you're not able to switch it out while you're still 10:54:52
processing the new rules. He said that's correct. And then 10:54:55
talking about once the compilation is complete, a signal is sent 10:54:58
to processer saying, hey, we're ready. It's done. He said 10:55:02
that's correct. And you can read the rest of the testimony. I 10:55:05
won't read it all into the record. I know we're on time. But 10:55:08
you can read this testimony and it syncs up exactly with the 10:55:11
claims. 10:55:15

Now Dr. Mitzenmacher showed you the Hitless ACL 10:55:18
documents. We showed you the data sheets, the white papers. 10:55:21
Mr. Jones' testimony is probably some of the best evidence 10:55:28
you'll see, and actually we'll see in the proposed finding of 10:55:31
fact. That's how we proved infringement by more than a 10:55:35
preponderance of the evidence of the DNA Center with the 10:55:38
Catalyst switches and the routers. 10:55:43

The next product offering was the Firepower firewalls 10:55:46
with the Firepower Management Center. Now if you look at how 10:55:49
this is configured, it's very similar to the switches and 10:55:53
routers. You see the Firepower Management Center as the kind of 10:55:56
the management center of all these different firewalls, and it 10:56:01
ingests threat intelligence. Now, this was an issue that I did 10:56:06
the cross-examination Mr. Shankar, and one of the things they 10:56:09

left out was Threat Intelligence Director, TID. I don't know if you remember that in their slides. I pointed that out, the Threat Intelligence Director is a new add-on to the Firepower Management Center that ingest these rules, ingests intelligence and then makes these rules and distributes them to the firewalls. 10:56:15 10:56:18 10:56:21 10:56:25 10:56:27 10:56:31

Now, Dr. Mitzenmacher -- 10:56:32

THE COURT: Now, do they do that before it reaches the destination? 10:56:34 10:56:38

MR. ANDRE: It creates the rule. The swapping is done down in the firewalls, but the rules are created up in the -- the ingestion of the rules are done in the management center. They're sent down, they're compiled, once you make the rules, you've got to compile them into a rule set and then put them into the system. 10:56:39 10:56:41 10:56:44 10:56:51 10:56:54 10:56:56

THE COURT: And once you've put them into the system it filters the packets before they reach the destination? 10:56:57 10:57:08

MR. ANDRE: That's correct. 10:57:13

THE COURT: Not afterwards? 10:57:15

MR. ANDRE: That's correct. And they can block packets that the rules say don't let through, and if the packet -- there's no rules to not let them through, they will let them through. It stops them before they get to the destination. This is the proactive, preventative technology that's in the routers and switches, it's in the firewalls as 10:57:15 10:57:18 10:57:21 10:57:24 10:57:26 10:57:30

well. 10:57:33

Dr. Mitzenmacher talked about you they ingest the 10:57:35 rules and the new rules are available and sent to the firewalls 10:57:37 and they perform a rule swap. 10:57:40

Now let me talk about the Threat Intelligence 10:57:42 Director. This is on slide 47. This is Exhibit 1289. It talks 10:57:44 about the Threat Intelligence Director ingests data from threat 10:57:51 intelligence sources and publishes it to all the devices it's 10:57:57 managing. And if you recall, when I talked with -- when it says 10:58:01 "The Threat Intelligence Director, after initial deployment of 10:58:06 access control policies to managed devices, you can configure 10:58:08 sources, indicators and observables without redeploying on the 10:58:12 system automatically." They automatically publish these new 10:58:16 data to the elements. And the piece of the testimony that I got 10:58:19 from Mr. Shankar during cross-examination was right on point. 10:58:21 Actually go back to that slide. I also want to point out one 10:58:25 other thing. 10:58:28

I'm sorry, in the figure on the left, this is what 10:58:28 Your Honor just asked. When a threat indicator incident is 10:58:31 fully realized, the system takes the configuration action, 10:58:35 monitor, block, partially block or no action. That's that 10:58:40 preventative, proactive stuff that we're talking about. So once 10:58:44 you put the rules in place on the firewalls, it can do all 10:58:48 these, it can monitor, it can block it, partially block, take no 10:58:51 action. 10:58:54

I took Mr. Shankar on cross-examination. So I said after the Threat Intelligence Director, after ingesting this threat intelligence, sends down the rules to the firewall, the firewall can take action to monitor, block, or partially block or take no action at all; is that correct? He says that's correct. And he gave an analogy which I really liked and I actually said I liked the analogy about the FBI Top 10 Wanted List, and that Top 10 Wanted List changes, it sends out new information, they can send it daily, they can send it hourly, and those new updates occur and they would occur on a very regular basis. And those are the automatic updates of the rules and rule swapping that's taking place in the firewalls. 10:58:57 10:59:00 10:59:04 10:59:06 10:59:06 10:59:09 10:59:13 10:59:17 10:59:20 10:59:23 10:59:26 10:59:31

What they call this in the firewalls -- and go to the next slide, something called the transactional-commit model. We showed you PTX-1196 and they defined the problem. They had, packets were being dropped during large compilations of rules and they wanted to avoid them. So they said "By knowing what's important to customers, we propose a transactional-commit model. With the legacy model, new rules will take affect immediately during compilation. In contrast with the proposed transactional-commit model, new rules will not take effect until compilation is done and stable. During compilation, packets will still match the old rules." So the use old rules until the get the new rules in place. Once you got the new rules in place, you do the swap. 10:59:34 10:59:37 10:59:42 10:59:47 10:59:51 10:59:55 11:00:00 11:00:04 11:00:06 11:00:10 11:00:12 11:00:16 11:00:19

Now we get to the next slide. This was from the 11:00:21
transactional-commit model. The key here is it prevents -- the 11:00:26
figure is not coming up here. 11:00:33

"It prevents packet drops while compiling large rule 11:00:34
sets during high traffic rate." So this is the key to the 11:00:37
transactional commit model. 11:00:41

Now for non-infringement purposes, what Cisco 11:00:43
attempted to do was -- and you probably recall this testimony -- 11:00:47
go to the next slide -- they said you had to reprocess the 11:00:50
processed packet. And you remember, you probably remember from 11:00:54
Dr. Reddy talking about this. He said you had to reprocess. 11:00:59
Dr. Reddy actually said -- and Your Honor asked him some 11:01:02
questions on this. This is at trial transcript 2635 13 through 11:01:05
2636, 11. He's saying that once you process a packet you have 11:01:09
to reprocess the packet. That was the basis for his opinions. 11:01:13
And it's just not the case. It was like that's not what happens 11:01:18
in the system and that's not what happens in the claim. The 11:01:23
claim was very clear that you don't process a packet with the 11:01:26
new rules until the new rules are fully in place and you can go 11:01:32
from there. And Mr. Hannah on cross-examination of Dr. Reddy, 11:01:35
he looked are at figure 4 from JTX-2 and actually showed that 11:01:38
that was not how it was done. That's not correct. And he 11:01:45
looked at it in figure 4 to show that Dr. Reddy's interpretation 11:01:48
of the claim was incorrect. 11:01:52

So with that, Your Honor, unless you have any further 11:01:55

questions, I will pass it to the other side and reserve a couple 11:01:57
minutes for rebuttal. 11:02:00

THE COURT: All right. Are you ready on cross? 11:02:01

MR. GAUDET: Your Honor -- 11:02:14

THE COURT: I mean for argument? 11:02:15

MR. GAUDET: Yes. I was on mute, Your Honor. 11:02:17

We will start on slide 41 of the Cisco binder. And 11:02:19
Your Honor, again, I think what we really have here is a basic 11:02:22
dispute about what the claim covers. As complicated as the 11:02:26
technology is, I think we probably agree on the most relevant 11:02:30
points. But what Centripetal is suggesting is that they have a 11:02:35
patent on the concept of not dropping packets. And if you 11:02:38
don't -- 11:02:42

THE COURT: Now wait a minute. What -- 11:02:43

MR. GAUDET: Slide 41, Your Honor. 11:02:47

THE COURT: Oh, I'm sorry. I was looking at 42. 11:02:49

MR. GAUDET: Yes. This is the claim language, and I 11:02:53
was going to, just before I get to the claim language I just 11:02:55
wanted to kind of give you some -- 11:02:58

THE COURT: All right. 11:02:59

MR. GAUDET: -- introductory remarks. 11:03:00

And that is, Your Honor, listening to Mr. Andre, 11:03:02
again, I don't know that on the material facts we have a big 11:03:04
dispute. This is really about what the claim covers. And 11:03:09
Centripetal's position seems to be that they got a patent on the 11:03:14

concept of not dropping packets during rule swaps, and as long 11:03:18
as you don't drop packets, you must infringe their patent. And 11:03:23
that is absolutely not what the claims say. The claims cover a 11:03:27
very specific way of not dropping packets during a claim swap, 11:03:30
and that's what I want to take you through, Your Honor. 11:03:36

This slide, slide 41, has the claim as they originally 11:03:38
filed it. We have seen this sort of thing before. And then on 11:03:44
the right-hand side is the claim as it was actually issued. And 11:03:48
what you can see is there is a lot of new language they had to 11:03:54
add. And I highlighted in red the language I'm going to focus 11:03:56
on in this argument. It was new. And it had to be added in 11:04:00
order to get this patent. And Your Honor, what this language 11:04:05
says is that a device is using its first set of rules. A second 11:04:08
set of rules arrives. And then -- this is so important -- the 11:04:14
first part that is in red, responsive to being signaled to 11:04:18
process packets in accordance with the second rule set. In 11:04:23
other words, in response to being told, hey, the second rule 11:04:27
set's here, the new rule set's here, you need to do something -- 11:04:30
in response to that signal. The way that they don't drop 11:04:33
packets is you now cease processing of packets and you cache 11:04:37
these packets. You do something different than what you were 11:04:41
doing before. And Your Honor, our basic non-infringement point 11:04:44
is it's definitely not that time stands still. That's not at 11:04:48
all what happens. It's that the processing of packets in all of 11:04:51
the accused systems happens on a regular interval. For example, 11:04:57

in the new products it's two clock cycles. And between every 11:05:01 packet that ever comes into the system, every -- this is 11:05:07 milliseconds -- every two clock cycles a packet is processed, 11:05:11 okay? It doesn't matter if the rule sets are being swapped or 11:05:15 not being swapped. And they have no idea if they have been 11:05:19 swapped or not being swapped. Every two clock cycles, a packet 11:05:22 moves out of the buffer and gets processed. And so there is 11:05:26 never something different. The fact that the rules arrived 11:05:31 don't cause a signal to say, hey, do something different with 11:05:37 respect to how you're processing, stop processing for a while or 11:05:41 take an extra pause. Nor is there a signal that says, hey, do 11:05:44 something extra or different with respect to the caching. And 11:05:48 that's what the claim requires. The way that this claim avoids 11:05:52 dropping packets is when the new rule arrives, instead of trying 11:05:56 to use it right away while it's getting it ready, okay, it 11:06:01 doesn't use the old rule set either. It caches the packets as 11:06:06 they're coming in, it stops processing, and then eventually it 11:06:10 starts again. 11:06:15

And the fundamental difference is that in our system, 11:06:15 we don't do anything different. The processing happens on 11:06:18 exactly the same cadence, and every witness said that, and 11:06:22 that's the testimony Mr. Andre put up, and the buffering, which 11:06:26 they're calling caching happens on exactly the same cadence. 11:06:29 There is no difference. And even if you were to find that 11:06:32 processing ceases during those two clock cycles, and even if you 11:06:39

were to find that buffering is the same thing as caching, none 11:06:42 of that happens in any way in response to a signal related to 11:06:46 the arrival of the new rule set. It happens. It doesn't -- the 11:06:51 buffering doesn't even know that there's been a new rule set. 11:06:57

And Your Honor, to explain why this matters, in the 11:07:00 prosecution history they tried to get, they -- there is a prior 11:07:05 art reference that was just keep on buffering as packets come 11:07:09 in, you know, that sort of thing, and the way this was 11:07:13 distinguished by Centripetal was to say in that prior art 11:07:17 reference, the queues, right, are configured to hold packets for 11:07:21 processing. That's just a standard buffer operation, just like 11:07:26 us. You're just waiting for processing. They say Nowhere 11:07:29 does -- that's the prior art name -- indicate that the queues 11:07:32 are configured to cache packets for which processing has ceased. 11:07:36 It's something different. 11:07:41

And Your Honor, their inventor said the same thing. 11:07:44 Dr. Moore, we've played -- this was about a four- or five-page 11:07:47 answer. We played the entire answer for you. I've got the last 11:07:51 part of it, but certainly invite you, the whole thing is in the 11:07:56 record, but he explained what the claimed caching is. It's not 11:07:59 just the same old process. It's something different. It's that 11:08:04 caching would be used in this sense. In the context for, oh, 11:08:07 those packets that you're already currently processing through 11:08:11 the old policy, you don't want to put those back on the buffer 11:08:14 from whence they were extracted in the first place. 11:08:18

If we go to the second paragraph. 11:08:21

You want to put them a higher-speed cache memory, so that once you're ready to start processing those packets again you can get to them as quickly as possible. 11:08:23 11:08:26 11:08:29

And the last part. Making sure you're securing those cache packets according to the new policy. The things that you -- it's not just business as usual, it's you have to do something new and different. And that's exactly what's missing. 11:08:32 11:08:35 11:08:40 11:08:44

So what's the proof of how we actually operate? And the truth is there's no disagreement. I didn't see any evidence Mr. Andre put up that was inconsistent with anything I'm going to tell you; that Hitless ACL updates, Mr. Jones says, it is applied to a given string of packets without disabling packet processing while the change is made. It just does exactly the same thing it was doing before. 11:08:48 11:08:51 11:08:54 11:08:56 11:09:03 11:09:06 11:09:09

Here in slide 46 he says in the answer, "It's a fixed time pipeline. There will be a packet every two or four internal clock periods" -- two with the newer ones, four with the older ones -- "and the switch happens between those." 11:09:11 11:09:15 11:09:19 11:09:21

And he showed this diagram and basically, you know, packets come in into the bottom, bottom left, and every -- in the newer ones, every two clock cycles, packet goes up to that top buffer and the header goes into this thing called the ingress-forwarding controller, all right? And it's processed and every two seconds it just keeps on happening, keeps on 11:09:25 11:09:28 11:09:33 11:09:38 11:09:41 11:09:44

happens -- sorry. Clock cycles, not seconds. Clock cycles. 11:09:51

Every two clock cycles that keeps on happening, and 11:09:55
then the middle green, the lookup tables, that's what gets 11:09:57
changed in between the two clock cycles. But the buffering and 11:10:00
the processing doesn't change in any way because of that. In 11:10:05
other words, there's nothing saying stop the processing, do 11:10:09
something different with the processing, start caching. There's 11:10:12
not even a signal. 11:10:15

And so when he was asked this question, bottom here, 11:10:17
"Please explain any relationship between the packet buffers 11:10:21
complex and the Hitless ACL rule update technique that we talked 11:10:24
about yesterday." "There is no relationship." 11:10:28

And I want to pull up the slide, Plaintiff's slide 43, 11:10:30
to show you what Mr. Andre pointed to from the same witness. 11:10:35
Because again, I think we're in complete agreement about the 11:10:38
facts. Your Honor, what I want to point to you is it's the 11:10:45
second-to-last row. This is where he has the testimony. But 11:10:48
what they have done is you've got to start reading before you 11:10:54
get to the second-last row in the claim language. Because it's 11:11:00
that phrase right before that says "configure each processor of 11:11:03
the at least two processors to, responsive to being signaled, to 11:11:07
process in accordance with the second rule set. In response to 11:11:13
a signal that the new rule set is here, you've got to do 11:11:17
something different. And what is the testimony on the right? 11:11:20
It just says, yeah, every two clock cycles, two or four, 11:11:22

depending on the product, we process a packet, and that's it. 11:11:27
And that's all it says. And during that break you swap from the 11:11:32
old to the new. We agree. That's not what the claim requires 11:11:36
though, Your Honor. The claim requires that something has to 11:11:39
happen in response to a signal that the new rule set arrived. 11:11:42
And that something is that you cease processing packets. You do 11:11:47
something about the processing and then you cache the packets in 11:11:51
response. 11:11:55

Let's go back to our slide set. 11:11:56

And the accused routers operate in exactly the same 11:12:02
way. And you know, Your Honor, what they're accusing here, this 11:12:05
basic buffering, the first part here is, that's -- I mean, the 11:12:09
process of buffering a packet before you process it, that's been 11:12:12
around since Cisco's inception. That's always the way you do 11:12:16
things. That's literally all they're accusing. The Patent 11:12:20
Office didn't give them a patent on that. 11:12:23

And Your Honor, the same thing for firewalls. The 11:12:26
same point in the firewalls. This is slide 50. And I want to 11:12:29
jump forward just a little bit here. The question, why is it -- 11:12:35
why does the patent cease processing and cache packets? What is 11:12:39
the purpose of this in the patent, to give this some context. 11:12:43
And this is in the background of the specification. They're 11:12:46
defining the problem. 11:12:49

THE COURT: Mr. Gaudet, you've got to pay attention to 11:12:50
the clock. You keep running over. 11:12:54

MR. GAUDET: Your Honor, I'm on 13 minutes, I believe. 11:12:58
I thought I had a 15-minute allocation. I know that Mr. Andre, 11:13:00
I think, may have -- but I thought I was on 13 minutes. I was 11:13:03
trying to pay attention to the clock and I thought I had 15. 11:13:06

THE COURT: All right. 11:13:11

MR. GAUDET: Your Honor, this is the final point here. 11:13:12
According to the background, the problem was that while 11:13:15
implementing a new rule set -- this is highlighted -- a network 11:13:20
protection device might continue processing packets with the old 11:13:23
rule set. In other words, after the new rule set arrives, you 11:13:27
might keep using the old one, and that's a problem. That's what 11:13:32
the patent solves by saying stop processing and cache. But Your 11:13:35
Honor, that's exactly what we do. That's how Hitless ACL works. 11:13:40
We keep using the old rule set. That's established by PTX-1293. 11:13:43

And the final point here, Your Honor, is you might ask 11:13:49
the question, why would you do that? Why wouldn't you do what 11:13:52
the patent does? And the answer is, from Mr. Shankar, it takes 11:13:56
several hours to get a new rule set ready, so spending an extra 11:14:00
couple minutes before you use it after it gets to the device is 11:14:05
just not that big of a deal. 11:14:07

We rejected the patent's solution. We do what the 11:14:09
patent distinguished. We do not, in response to the arrival of 11:14:13
a second rule set, of a new rule set, do any ceasing of 11:14:17
processing or any caching. 11:14:20

And Your Honor, that's all that I have on this one. 11:14:23

MR. ANDRE: Your Honor, I'll just use a minute or two 11:14:32
so we can get back on schedule here. 11:14:34

If we go back to slide 43? 11:14:35

This is the testimony from Mr. Jones. I know Your 11:14:38
Honor saw this testimony. Mr. Gaudet says there's nothing that 11:14:41
says stop processing packets. If you look down to the fourth 11:14:44
box on the right-hand side there's a question, "But there's a 11:14:51
signal that says stop processing packets with the old rule set 11:14:54
and start processing packets with the new rule set, correct?" 11:14:57

"Yes. We swap the old to the new." And you do that 11:15:01
swapping between, in between those clock cycles you mentioned. 11:15:04
That's when the packets are being stored in the buffer. So Mr. 11:15:07
Gaudet says there's nothing they stop processing packets. We 11:15:10
got direct testimony of Mr. Jones that says that, and we showed 11:15:14
him documents that showed the exact same thing. In fact, there 11:15:17
is a signal that says stop processing packets while you switch 11:15:23
out the rules. 11:15:26

THE COURT: Okay. 11:15:30

MR. ANDRE: Your Honor, I'll let Mr. Hannah take over, 11:15:32
and he's going to be doing the '205 patent now. 11:15:33

MR. HANNAH: Thank Your Honor. May I proceed? 11:15:43

THE COURT: Yes. 11:15:45

MR. HANNAH: Thank you. 11:15:47

So the '205 patent, this is again one of the patents 11:15:47
covered by Dr. Mitzenmacher. This patent talks about providing 11:15:50

dynamic security policies to a variety of network devices. And this is what allows for the processing of the SIP traffic and the encapsulation. That's what this patent specifically talks about. And we heard a lot of testimony about this. 11:15:55 11:15:58 11:16:01 11:16:07

Next slide we see Dr. Mitzenmacher again provided a number of exhibits, and in this, for this scenario it's similar to the '806 in that we have both the switches and the routers with DNA, that's one contention, and then the firewalls plus the Firewall Management Center as the other contention. And so I'll start with the switches and routers with the DNA Architecture. 11:16:09 11:16:12 11:16:15 11:16:20 11:16:25 11:16:29

So we turn to that, it's a similar slide Mr. Andre just showed, but what we're focusing on here is we have the DNA Center that's going to be processing these different rules and these different processes, these dynamic policies and pushing them down to the Catalyst switches, the routers and the Aggregated Services Routers and the Integrated Services Routers. 11:16:34 11:16:36 11:16:41 11:16:44 11:16:47 11:16:51

We turn to Dr. Mitzenmacher's opinion and we see that, again, he says the Catalyst 9000 switches and all the routers with the DNA, they infringe the '205. The DNA Center is a security policy management server, and we showed a number of documents, and we'll show a couple this morning, that sends policies to the switches and routers. These switches and routers, they enforce the policies, and that includes enforcing rules that process SIP traffic. And we showed a number of documents in which they process SIP traffic. 11:16:55 11:17:00 11:17:03 11:17:07 11:17:10 11:17:13 11:17:15 11:17:20 11:17:23

We also showed a number of documents in which encapsulation is performed, and that's the last element that's provided here. And that's done through this thing -- one of the ways that this is done is through tunneling. And we explained where that tunneling is, and you rewrite the header of the packet, you send it through this tunnel so you can process it at the other end of tunnel. 11:17:25 11:17:28 11:17:32 11:17:36 11:17:39 11:17:42 11:17:45

So starting with the policies, the dynamic security policies from the security policy management server. That's the DNA. And it says in 1294, PTX-1294, you create these policies, you allow the creation of policies based on business intent for the particular part of network, and these configurations can be adjusted dynamically based on the network conditions. These are the dynamic security policies that we're talking about with the '205 patent. 11:17:48 11:17:50 11:17:55 11:18:01 11:18:05 11:18:07 11:18:11 11:18:15

If we go to the next slide, we talked about how the DNA Center is going to be sending these policies to the switches and we showed how, that the switches have the ability to process SIP traffic. There's a lot of testimony, and the highlighting looks like it's a little off here, it should be highlighting the SIP traffic for the voice phones here. And there was a lot of -- there was some testimony which we'll look at later that they do this for security purposes; that the switches and routers, they don't look at SIP for security at all, that it's done for monitoring phone calls. That's not what their 11:18:18 11:18:22 11:18:25 11:18:31 11:18:34 11:18:37 11:18:40 11:18:44 11:18:47 11:18:51

documents say. You look at their technical documents, it says that they have SIP traffic and they do it for security purposes. 11:18:55 11:18:58

We also showed you a number of documents about encapsulation for the switches and routers. 11:19:02 11:19:03

THE COURT: Wait a minute. Let's look at that last one. Where does it say security? 11:19:07 11:19:08

MR. HANNAH: At the very top, Your Honor. So it's Advanced IOS Security. This is an overview. And then it talks about how you have data plane security and control plane security. And then the highlighting got moved, it looks like, but the, if you look under the fifth bullet point, or it's the second one underneath the Data Plane Security, the second small bullet point -- there you go. Thanks, Geoff -- SIP traffic for phones, part of the data plane security that we're talking about here. And this is the same operating system that works on the switches and routers that we've talked a lot about over the weeks. 11:19:10 11:19:13 11:19:16 11:19:19 11:19:24 11:19:28 11:19:36 11:19:40 11:19:44 11:19:48 11:19:51

We showed you PTX-524 as an example of encapsulation, the switches an routers they can do condition. They do this for a variety of reasons. Again, it's for these tunneling reasons, it's able to be able to create these protocols so that you can send these packets to another destination for a variety of purposes. If you have two offices, if you want other monitoring or processing. We showed you a number of these encapsulation documents. 11:19:51 11:19:57 11:20:01 11:20:04 11:20:08 11:20:11 11:20:15 11:20:19

THE COURT: You can send it to other destinations. Do you block it from going to its original destination with this technology? 11:20:19 11:20:21 11:20:26

MR. HANNAH: You reroute it from going from its original destination through the tunnel. Absolutely, Your Honor. At the other end of the tunnel you can determine whether you want to block it at that point or you can allow it to go to its destination, or you can do whatever you want through the tunnel. But the point -- 11:20:27 11:20:32 11:20:34 11:20:36 11:20:39 11:20:42

THE COURT: Before it reaches the destination? 11:20:43

MR. HANNAH: Absolutely. That's what encapsulation is all about. It is that you change the header of the packet so you send it through the tunnel, and then once you do that, it diverts it from its -- routes it from its original destination to the, through the tunnel. And if you look, Your Honor, it says Encapsulations, Generic Routing Encapsulation, it talks about how you do this routing through the tunnel. 11:20:46 11:20:48 11:20:52 11:20:56 11:21:00 11:21:05 11:21:09

THE COURT: Well, if you're tapping a telephone with this technology, if it doesn't go to its original destination, what is there to tap? 11:21:13 11:21:15 11:21:23

MR. HANNAH: That's, it's not -- this patent is not about tapping telephones. That's what the defendants are trying to characterize it as. It's about providing security. What happens is, you have bad actors who can send malicious traffic through the SIP traffic. So you think it might be a SIP, it 11:21:25 11:21:27 11:21:31 11:21:35 11:21:40

might be a phone call, it might be, you might think it's VoIP 11:21:45
traffic, and so you don't inspect it at all and it's allowed to 11:21:51
go through. The malicious actors have targeted that vector. So 11:21:53
now that's exactly why that last document I just showed you, you 11:21:58
have to apply security to that vector. It's not just a phone 11:22:02
call. It's another road that they can get into your network. 11:22:07
And so that's what the '205's about. It's about providing 11:22:13
security over that channel. It's not about monitoring phone 11:22:17
calls. That's the mischaracterization that we've got from the 11:22:21
defendants. And as I show later in slides, their expert 11:22:26
actually made the affirmative statement that the '205 is not 11:22:33
about security at all. And if you look at the claims, you look 11:22:35
at the title, you look at the title of the patent, it talks 11:22:38
about security. 11:22:41

So I'd like to just move quickly to the firewalls and 11:22:44
the Firepower Management Center, and it has the same 11:22:49
functionality. We look at the architecture. It's the Firepower 11:22:52
Management Center. It receives this threat intelligence and 11:22:57
pushes these policies to all of the firewalls. Dr. 11:22:59
Mitzenmacher's opinion was similar for the firewalls. 11:23:03

If you go to the next slide, specifically it shows 11:23:06
that you have these firewalls, they had Firepower Management 11:23:09
Center that is the security policy management center. It sends 11:23:12
these policies to the firewalls. The firewalls enforce these 11:23:15
pollices. They provide security. And they process the SIP 11:23:19

traffic. And then the firewalls have the capability to encapsulate those packets via this tunneling. This is shown in the documents. 11:23:22 11:23:26 11:23:29

You look at PTX-1289, it talks about how you have security intelligence -- this the Threat Intelligence Director -- and you have these policies that are created to form these IP addresses, URLs and domains, and you can send these policies without requiring redeployment. That's the dynamic nature of these policies. 11:23:30 11:23:34 11:23:35 11:23:40 11:23:43 11:23:49

Let's go to the next slide. I think this is actually going to really help, Your Honor, and answer your specific question. It's not about monitoring phone calls. Look at the highlighting here for SIP keywords. It says "Four SIP keywords allow you to monitor SIP session traffic for exploits." For security. You're not tapping phones. You're not trying to say, you know, see what's going on. You're looking at the SIP traffic because it's a hidden vector, it's another road that attackers can use because you think it's a phone call. It's an exploit. And that's what this firewall does. It looks at the SIP traffic and tries to see, okay, is this going to be malicious? 11:23:51 11:23:53 11:23:56 11:23:59 11:24:03 11:24:07 11:24:12 11:24:16 11:24:20 11:24:24 11:24:28 11:24:31

And right here on this slide it also -- this is PTX-1289 -- it shows an example rule that's used to look at the SIP header and match the field. You alert if you have any of these suspicious kind of operations that are going to be 11:24:31 11:24:33 11:24:38 11:24:43

happening, and you are going to be able to alert and react to 11:24:45
those and block that traffic. 11:24:50

That's exactly what the next slide shows. It's the 11:24:52
same document, this document shows all these features. You 11:24:54
extract the SIP header and you pass the -- you pass it to the 11:24:58
rules engine for further inspection. You don't monitor the 11:25:03
phone call, you look at the SIP header, you look at the traffic 11:25:06
and look at the rules to say, okay, let's inspect this traffic 11:25:10
for security purposes. 11:25:13

The firewall in PTX-1293 also has this capability of 11:25:16
performing the tunnel. This is the encapsulation we're talking 11:25:21
about. It specifically says you have a secure connection. 11:25:25
"It's called the tunnel. The ASA uses these tunneling protocols 11:25:29
to negotiate security, create and manage tunnels and encapsulate 11:25:32
packets, transmit them through the tunnel and then unencapsulate 11:25:38
them." That's what the firewall had the capability of doing. 11:25:42

THE COURT: Well, when you encapsulate it, does that 11:25:44
stop it from reaching its destination? 11:25:48

MR. HANNAH: It does, Your Honor. It'll send it 11:25:50
through the -- instead of going to the destination, it diverts 11:25:51
it, it routes it going to the, to the tunnel. And it has to do 11:25:54
that by changing the header. 11:25:59

THE COURT: Where does it go? 11:26:01

MR. HANNAH: It can go whenever you want it 11:26:03
programmed. It can go to another end to do some work, to 11:26:05

monitor -- I mean to enforce or to look at the traffic some 11:26:09
more. You can go, you can send it to, if you had a corporation 11:26:12
or another office, you might want to send it over there, might 11:26:15
have some higher processing. But all the claims require is the 11:26:19
ability to encapsulate this traffic and be able to send it 11:26:23
through these tunnels and provide the security function. 11:26:27

If you look at the next slide, this is the claim set, 11:26:32
and their non-infringement arguments are largely based on 11:26:36
rewriting the claims again. First, you have a single rule that 11:26:40
specifies a set of network addresses. That's just a plain 11:26:47
rewrite of the rule, at least one rule. 11:26:52

And then they have this argument that you have to have 11:26:54
SIP colon in the rule. 11:26:56

If we turn to the next slide, this was debunked during 11:26:59
cross-examination. During cross-examination, we showed him the 11:27:04
plain language and it says "The asserted claims do not require a 11:27:07
single rule, correct." 11:27:09

"No, there can be multiple such rules based on the 11:27:10
claim language." 11:27:13

We also debunked the fact that you have to have SIP in 11:27:14
the rule itself. You look in the specification, we showed this. 11:27:17
This is on column 14. It specifically has an example of a SIP 11:27:22
URI and it does not include the SIP colon. That's because you 11:27:29
don't need that for security purposes. For security purposes, 11:27:32
you just need the information necessary to determine if it was 11:27:35

coming from a bad place. 11:27:38

Now as I alluded to earlier, we talked about Dr. Jeffay's trial testimony, and his entire testimony was based on this monitoring phone calls and that the -- and he was asked, this is on redirect, "With respect to No. 5, risk mitigation with multiple security, is the '205 patent even about security?" 11:27:40 11:27:42 11:27:45 11:27:50 11:27:53

"No, no, it's about helping law enforcement." 11:27:57

This goes largely to his credibility. You look at the claim language. The claim language is absolutely the '205 is about security. 11:28:00 11:28:03 11:28:07

Go to the next slide. 11:28:08

A security policy management server. Of course the '205 is about security. A packet security gateway. That is what the routers, switches and firewalls are acting as. And they have dynamic security policies. So his notion that you don't have security, it completely cuts against the credibility and shows that the '205 is infringed by those products. 11:28:09 11:28:12 11:28:16 11:28:20 11:28:24 11:28:29

THE COURT: So are you accusing the firewalls as well? 11:28:32

MR. HANNAH: Absolutely, Your Honor. The firewalls is what I just showed where it has the SIP headers that get extracted from exploits. So it's the routers and switches plus DNA and then the firewalls with the Firepower Management Center. 11:28:36 11:28:38 11:28:41 11:28:44

THE COURT: Okay. Cross-examination? He used up most of the time. 11:28:50 11:29:00

I keep saying cross-examination. Response? 11:29:01

MR. GAUDET: Yes. Your Honor. 11:29:07

THE COURT: After six weeks of cross-examination... 11:29:09

MR. GAUDET: Let's go to Slide 61. And Your Honor, 11:29:12
after six weeks, this is now the third patent that I think we 11:29:14
fundamentally have a disagreement about what the patent covers. 11:29:19

Your Honor, just, this is -- actually let me go back 11:29:23
to slide 59 here. 11:29:28

Your Honor, you're exactly right. And Dr. Jeffay laid 11:29:32
it out that what this claim covers is wire tapping. You have to 11:29:36
send, according to the claim, and I'll get you there, you have 11:29:40
to send the original packet all the way to the end, otherwise 11:29:42
there's nothing to wire tap. Now I'll walk you through the 11:29:47
claim. 11:29:50

Mr. Hannah did something sort of interesting in trying 11:29:50
to argue why it was that the patent, the patent covers blocking 11:29:52
and security in the form of blocking. He went to our accused 11:29:59
products and said see in the accused products, there's no 11:30:02
tapping. There's blocking, and we agree with that, but that's 11:30:05
why we don't infringe. 11:30:09

Your Honor, the language from the specification here 11:30:11
talks about exactly what happens in figure 6. It's this law 11:30:13
enforcement scenario. And this is now figure 6. What we have 11:30:16
up here is this reflects the ability -- this line here, is just 11:30:21
the ability of processing SIP traffic that's been around for 25 11:30:27
years. Upper left, there's a phone call made from that user 11:30:30

equipment device, it goes over the Internet, it lands at the 11:30:34
user in the bottom right who has got this, effectively, phone 11:30:38
number which is this SIP URI there in the payload. That's been 11:30:42
around for 25 years. 11:30:48

This is what the patent changes. It stops that call. 11:30:50
If it matches with the SIP URI who you want to wire tap, you 11:30:53
encapsulate it. But it's not enough just to encapsulate. The 11:31:02
claim requires a lot more. And I highlighted in red the lot 11:31:05
more, Your Honor. After you encapsulate it, you send it down to 11:31:09
this network device that's in the bottom left. You have to copy 11:31:13
the information and then you forward it to the original 11:31:18
destination called the Destination Network Address. You cannot 11:31:23
block it. You have to forward it. If you block it, you cannot 11:31:26
possibly satisfy this claim. And it's just that simple. And 11:31:30
everything he's accusing is blocking. Is stopping the phone 11:31:34
call. 11:31:37

And then the last element is that you route, you know, 11:31:38
you actually carry out this routing to the monitoring device. 11:31:41
Your Honor, this wasn't some minor thing. We've got here on 11:31:45
slide 63, this was a big part of the reason that the Patent 11:31:54
Office allowed the claim. In the Notice of Allowance the 11:31:57
examiner literally quoted everything to the bottom of this 11:32:02
slide. Beginning with the "encapsulate at least one packet", 11:32:05
they quoted everything in element E down to "network address 11:32:08
with copy and forward." And they said this is why you're 11:32:14

different. This is why you're different than the prior art. 11:32:16
You're not just processing SIP traffic. And they didn't even 11:32:18
try to satisfy this. 11:32:25

And Dr. Jeffay pointed out, Dr. Mitzenmacher and now 11:32:25
Mr. Hannah never suggested this process of encapsulating, 11:32:29
sending it to a device that copies and then forwards. And 11:32:35
that's a very specific thing. It would require a bunch of 11:32:39
equipment and a bunch of engineering and a bunch of software, 11:32:42
and they have never pointed to anything. Mr. Hannah generally 11:32:44
said there's encapsulation and then took this leap that 11:32:48
therefore there must be every other claim element with 11:32:51
absolutely no evidence. And Dr. Mitzenmacher didn't even try. 11:32:56

I think it's clear Dr. Mitzenmacher is accusing the 11:32:59
blocking of packets. That's slide 65. He said it again in 11:33:03
Slide 66. And this is now Slide 67, Dr. Jeffay's explanation. 11:33:08
He said it's not about blocking packets. Because if you block 11:33:16
packets, intuitively there's no call to tap, and you obviously 11:33:20
are not forwarding the original packet to its destination, thus 11:33:24
it's literally the opposite of the claims. 11:33:34

The other thing with respect to the doctrine of 11:33:37
equivalents, Dr. Mitzenmacher said that blocking would be 11:33:39
equivalent to what the claim requires. Blocking is the opposite 11:33:45
of what the claim requires. But beyond that, Your Honor, for 11:33:50
this and for the other patents that were involved in 11:33:55
prosecution, when they had to add these elements or make 11:33:58

statements about them, there can be no doctrine of equivalents. 11:34:02
You don't get to use the doctrine of equivalents on elements 11:34:03
that you had to add in order to overcome prior art. 11:34:06

The second point, Your Honor, and I'll just, I'll be 11:34:12
very brief on this one, it's just the point about what a SIP URI 11:34:14
is. And this is the second independent reason. And I think the 11:34:18
punch line here is, as Dr. Jeffay explained, the SIP URI has to 11:34:24
identify somebody specific. Because what they're saying is it's 11:34:30
just a domain name, it's just unc.edu. And that's just not good 11:34:33
enough. And Your honor, I think I'm going try to save us some 11:34:38
time. That's everything that I have. 11:34:41

THE COURT: All right. Any rebuttal? 11:34:45

MR. HANNAH: Just briefly, Your Honor. 11:34:50

If we go back to slide 66 from our slide deck. 11:34:50
Counsel tries to say that the evidence that we point to, 11:34:54
everything says that you're going to block. And I just want to 11:34:57
point out what the documents actually say. 11:35:01

Says "Four SIP keywords allow you to monitor the SIP 11:35:03
session traffic for exploits." 11:35:07

If we go to the -- talks about monitoring for it. 11:35:08

And if you go to the next slide, and this is 11:35:11
deliberate, if you look at Slide 67, "You extract the SIP header 11:35:14
when present and passing it for further inspection." 11:35:18

So this whole notion that we're requiring blocking 11:35:21
that's in the products and that the products only block and they 11:35:26

don't do inspection, is just contrary to the documents. 11:35:29

With that, Your Honor, unless there's any further 11:35:33
questions, we can move on to the next patent. 11:35:35

THE COURT: I think we actually move on to a recess. 11:35:39

MR. HANNAH: Yes, Your Honor. 11:35:41

MR. GAUDET: Mr. Hannah and I teamed up to actually 11:35:45
get ahead of schedule a little bit, Your Honor. 11:35:47

THE COURT: You did. You're five minutes ahead. So 11:35:50
we'll take a recess until -- well, this says we'll resume at 11:35:54
11:40. 11:36:04

MR. GAUDET: I think we were going to stop at 11:40. 11:36:09

THE COURT: Yeah. We're going to stop at 11:40. 11:36:14
Right. We'll take a recess until 11:55. 11:36:15

MR. GAUDET: Thank you, Your Honor. 11:36:22

(Recess taken from 11:37 a.m. to 11:57 a.m.) 11:36:23

THE COURT: All right. We are on the '856 patent. 11:57:42

MR. ANDRE: That's correct. The '856 patent. May I 11:57:47
proceed? 11:57:54

THE COURT: Yes. 11:57:54

MR. ANDRE: Your Honor, as you know, the '856 patent 11:57:54
is the one we call the encrypted traffic patent, the detection 11:57:56
of network threats in encrypted traffic without decrypting using 11:58:00
threat intelligence and using the unencrypted portion of 11:58:05
encrypted packets to determine that there are threats. 11:58:10

Dr. Eric Cole was our expert on this case. There's a 11:58:13

nice picture of Dr. Cole, not the mugshot. And he showed a lot 11:58:16
of exhibits to prove the infringement case. 11:58:20
Now if we go to the next slide, PTX-989, this was kind 11:58:24
of the base foundation of Dr. Cole's testimony. This is the 11:58:28
system that we're talking about. And if you look at it, it's 11:58:33
called the ETA Solution with the Catalyst 9K. That's the title 11:58:38
of this. And this is PTX-989 at Page 33. Has the Catalyst 9000 11:58:41
series switches with the ETA on them. It sends NetFlow exports 11:58:48
up to StealthWatch, StealthWatch has ETA as well, and the 11:58:53
Cognitive Threat Analytics, it also see on the right-hand corner 11:58:58
it gets Threat Grid, it gets third-party threat intelligence as 11:59:00
well. It does analytics up in the Cloud up there in the 11:59:04
Cognitive Cloud and determines what are threats and what are not 11:59:08
threats, it then sends that information over to the Identity 11:59:12
Service Engine, the ISE on the left-hand side, and then the 11:59:15
Identity Service Engine can send rules down to the Catalyst to 11:59:19
say what's good and what's bad and what it should block and what 11:59:22
it shouldn't block. That's the COA, the Change of 11:59:25
Authorization. 11:59:29

Now, Dr. Cole's opinion with respect to this system 11:59:29
was that the 9000 switches and ASR and ISR routers embedded with 11:59:33
ETA working with StealthWatch, which is integrated with ETA and 11:59:38
CTA, the Cognitive Threat Analytics, and Identity Service 11:59:42
Engine, infringe the '856 patent. 11:59:42

It's important to note the infringing system receives 11:59:48

data indicating network-threat indicators including a domain 11:59:51
name. That's the threat intelligence feeds from the third 11:59:51
parties and from others up in the Cloud. They also get it from 11:59:56
the initial data packet. They get filtering out when packets 11:59:59
are coming through. This is the IDP also provides threat 12:00:03
intelligence. That's at the switch and router. They also get, 12:00:07
as I said, StealthWatch through the third party. 12:00:11

The switches and routers identify packets that include 12:00:13
unencrypted and encrypted data. They perform the initial of 12:00:17
these packets initially based on the Uniform Resource Locator, 12:00:19
which is that domain name, and protocol version. So when the 12:00:21
packets come through you get initial filtering, and then a 12:00:26
representations of those packets are sent to StealthWatch for 12:00:31
additional filtering and analysis. That's the NetFlow data that 12:00:32
we've heard so much about. 12:00:36

The infringing system then can route packets that are 12:00:37
determined to comprise data that correspond to network threat 12:00:42
indicators to a proxy. In this case it's a null interface. 12:00:46
That was Dr. Cole's opinion. He provided that opinion in a 12:00:48
narrative on the next slide that I showed you, I believe it was 12:00:53
yesterday or the day before. Sometime this week. I've lost 12:00:58
track of time. This was Dr. Cole's testimony. And he also, he 12:01:01
did it with the -- a system that we showed earlier, and he also 12:01:05
did it here. He talks about how the whole system is infringing 12:01:10
this claim. 12:01:13

Now, if we go back to that figure and annotate it, and 12:01:15
Dr. Cole actually talked about this and that previous slide 12:01:20
talked about this, he says he used badguys.com as an example of 12:01:23
a bad site. So if badguys.com is identified as a bad actor, the 12:01:28
threat indicator said this is bad, that badguys.com is sent over 12:01:37
to the Identity Service Engine to say this is a bad site. The 12:01:43
Identity Service Engine will then write a rule and send that 12:01:47
down to the switches or routers saying block badguys.com, don't 12:01:50
let it get to its intended destination. So when badguys.com 12:01:55
comes into that switch and router, switch or router, that rule 12:02:00
is in place, it's going to drop the packet, dump it, put it in 12:02:04
the null interface. You have to route it somewhere. You have 12:02:08
to route it to a proxy, and it has to be delivered there, 12:02:11
otherwise badguys.com will keep sending that in perpetuity. You 12:02:14
have to have a destination it reaches. That's the reason you 12:02:18
have to send it to a proxy. That testimony went largely 12:02:20
uncontested. 12:02:24

We showed you deposition testimony of principal 12:02:25
engineer at Cisco, Sunil Amin. It says "Would StealthWatch send 12:02:30
a message to the Catalyst switches?" 12:02:35

Said "I believe that's true. And in responding to 12:02:36
that message from StealthWatch, may route a package in a 12:02:40
particular way. 12:02:43

Said "In what way would the Catalyst switch route 12:02:45
packages based on a message from StealthWatch? 12:02:47

"Example, "drop packets, i.e., not forward them." 12:02:48

So StealthWatch sends a message, it goes the Identity Service Engine and it gets down to the Catalyst switches. 12:02:52 12:02:53

We also showed in the trial testimony, Mr. Llewallyn, it says "It may be used as part of an attack in the future. Do you see that line?" 12:02:57 12:03:00 12:03:09

"Yes." 12:03:10

"So the host is quarantined off the operator, then in the future, yes, the bad guy can't reach him." 12:03:11 12:03:11

And you say "What stops the bad buy," is the question from the Court. "Where is he stopped, and by what means?" 12:03:16 12:03:18

Mr. Llewallyn says "What happens is the ISE," the Identity Services Engine, "it talks to the switches and routers in the Enterprise." Said he didn't know a whole lot about it, but big picture, it causes it be routed to a space that causes no harm." 12:03:21 12:03:24 12:03:27 12:03:31 12:03:31

"What causes it to be routed to a space?" 12:03:34

"This Identify Services Engine, when you issue the quarantine operation -- actually, from my understanding, reconfigure the switches and routers to say for this particular host, if someone is trying to reach this particular host, send them over to a different place that doesn't matter. They call it the null zero. That's the null interface. It just drops the packets." 12:03:37 12:03:38 12:03:41 12:03:44 12:03:47 12:03:50 12:03:54

That's what their engineer talked about. 12:03:55

Dr. Cole actually showed testing I thought that was -- 12:03:57

THE COURT: Wait a minute. Let me look at that last 12:04:05
one. 12:04:07

MR. ANDRE: This is Slide 82 on our deck. It just 12:04:15
drops the packets. So -- 12:04:21

THE COURT: Okay. 12:04:23

MR. ANDRE: -- Dr. Cole, being the kind of 12:04:23
cybersecurity guy he is, he wanted to do his own test on this. 12:04:28
So he actually did. Showed the Court a series of tests he did. 12:04:30
On the left he had the Encrypted Traffic Analytics, turned on 12:04:34
the switch that he was testing. He went to badguys.com. And 12:04:38
you can see that there is all the information that was picked up 12:04:43
from badguys.com. It even got the domain name. It shows 12:04:48
badguys.com in the bottom right blue box. Actually picked up 12:04:53
the domain name. That's the filtering it does after it gets to 12:04:56
the switches and routers. If there's a rule that said 12:04:59
badguys.com should be blocked, at that point it will route it to 12:05:02
the null interface. He turned ETA off and you see what showed 12:05:05
up. Nothing. The badguys.com just went through. It was not 12:05:08
detected. Not determined what was encrypted and what was not 12:05:12
encrypted. It was not reading and doing that filtering at the 12:05:16
switch and router at that point. Dr. Cole testified to that to 12:05:20
his testing. 12:05:24

Now, we go to the next slide. We go to PTX-584, this 12:05:25
is one of the exhibits you used about StealthWatch. Talked 12:05:28

about StealthWatch maintains a Global Risk Map. It's a behavior profile. This is that third-party threat feeds it gets. Global Risk Map and Encrypted Traffic Analytics data reinforces using advanced security analytics. It says "Upon discovery of malicious encrypted flow can be blocked or quarantined by StealthWatch. It does that by going through the Identity Service Engine and blocking it at the switch and router." That's what Dr. Cole talked about. 12:05:31 12:05:35 12:05:39 12:05:43 12:05:46 12:05:50 12:05:52 12:05:54

Going back to Mr. Llewallyn's testimony at trial, he also reaffirmed this. Said "Now StealthWatch working with other products and Cisco's security suite, in this case the Identity Services Engine, can proactively protect against threats, correct?" 12:05:58 12:06:01 12:06:06 12:06:08 12:06:11

Said, "Well, it's based on manual operations though. 12:06:12

"But it's on the code. The computer can do it, right? 12:06:15

"Yes. It provides a way to quarantine the host by clicking a button. You can address those threats faster. Both proactively with threat detection and retroactively with advanced forensics; is that correct? 12:06:17 12:06:20 12:06:25 12:06:29

"That's correct." 12:06:31

You can do it proactively, you can block the threat proactively, they get through, you can do it with, retroactively by advanced forensics as well. 12:06:31 12:06:35 12:06:38

The key to all this, one of the keys, along with analytics, was ETA flow records. This was added in in 2017. 12:06:40 12:06:44

The flow records were modified, the NetFlow was modified to 12:06:51
allow the initial data packets, the Sequence of Packet Lengths 12:06:55
and Times and other aspects that you would get in the flow 12:06:56
records, and the Initial Data Packet that contains mostly 12:07:02
protocol related to data in headers such as Service Name 12:07:05
Indicators, the SNI. That's the domain names we're talking 12:07:08
about. Protocol versions and other things that you can see 12:07:12
there. So when they added in ETA flow records, that allowed 12:07:14
them to start looking at the encrypted traffic at the switches 12:07:18
and routers and being able to start filtering them out and doing 12:07:22
threat determinations on this type of encrypted traffic without 12:07:26
decryption. 12:07:29

Now if we go to the next slide, this was once again 12:07:31
more confidential technical documents from Cisco. If you look 12:07:35
at the left, they're striking the balance. They say "The 12:07:39
industry's first network with the ability to find threats in 12:07:43
encrypted traffic without decryption." That's key. That's part 12:07:47
of the claim language. You're looking at the unencrypted 12:07:49
portion. "Secure and manage your digital network in real time, 12:07:53
all the time, everywhere." They do it proactively. They do it 12:07:56
in real-time. 12:08:00

And it talks about "We enhanced the network's sensor 12:08:03
to detect malicious patterns." So they've taken the switches 12:08:08
and routers and now they are sensors. They're just not switches 12:08:11
and routers, they have fundamentally changed what they do with 12:08:16

the Catalyst 9000 and the new operating system. 12:08:19

How does ETA work? It looks at these three elements. 12:08:23
The Initial Data Packet, which we talked about, the Sequence of 12:08:27
Packet Lengths and Times, and the Threat Intelligence Map. 12:08:30
That's that third-party global stuff. So they use all three of 12:08:36
this and the analytics to figure out what's good and what's bad. 12:08:39

If you look at the Global Risk Map, this is what it's 12:08:46
referring to. You can see here they talk about "We model and 12:08:49
use 20 features of 150 million malicious risk and 12:08:53
security-related events." They talk about they use the domain 12:08:56
data. The feature includes domain data, Whois data. That is 12:08:59
absolutely what's required. 12:09:04

Mr. Llewallyn confirmed when we talked about the 12:09:04
Global Risk Map, "So the second paragraph talks about, 12:09:08
"StealthWatch maintains a Global Risk Map, a very broad behavior 12:09:11
profile about servers on the Internet, identifying servers. Do 12:09:16
you see that? 12:09:19

He says "Yes." 12:09:19

"It identifies the bad guys out there, StealthWatch 12:09:19
does, that may be used as an attack in the future, right? 12:09:23

"That's correct." 12:09:26

So this is information that is going to be used by a 12:09:27
potential attack in the future. The proactive behavior we're 12:09:31
talking about. 12:09:34

Now, Dr. Schmidt's testimony regarding 12:09:34

non-infringement is that he believed that the claim required 12:09:40
that it be a decryption of the packets. He rewrote the claim. 12:09:43
Simply the patent goes further and requires the ability to 12:09:47
decrypt information. So you see the red language in that bottom 12:09:50
claim? That's what he added in. Instead of just routing by the 12:09:54
packet filtering system to the proxy, once it gets in the proxy 12:09:57
it has to decrypt the packets, and that's just not in the claim. 12:09:59
His entire non-infringement opinion is based on that. 12:10:03

You also -- Dr. Schmidt's credibility was, I think, in 12:10:06
severe jeopardy. He talked about that when we showed him this 12:10:09
document how the switches and routers can detect and stop 12:10:14
threats before, during and after, and I asked him, I said it's 12:10:17
your opinion detect and stop threats, does that mean detect and 12:10:21
stopping threats before they get the host? He said it's not 12:10:25
clear. Wasn't sure about it. 12:10:27

And lastly, Dr. Schmidt's credibility has to be called 12:10:29
into question as well because when we talked about the issue of 12:10:32
real-time and catching them in the act, when he say real-time 12:10:34
does not mean real-time, it means two to four hours. Your 12:10:39
testimony is between two to four hours. He said yes. I showed 12:10:43
him a document and said, well, here it says real-time detection 12:10:46
of attacks by immediately detecting malicious connections in a 12:10:50
local environment. I said so does the word immediately chance 12:10:51
your sentence [sic]? He said, again, immediately is always 12:10:55
relative to something. Also said about catching them in the act 12:10:59

doesn't mean catching them in the act, it means catching them 12:11:02
after the fact. I used my analogy of breaking into my house and 12:11:04
stealing all my jewelry and furniture and such, and he said 12:11:08
yeah, that's catching them in the act if they catch them two 12:11:12
weeks later. So I think Dr. Schmidt's credibility is severely 12:11:15
called into question on this one. 12:11:19

And that's all I have, Your Honor. I'll save the rest 12:11:20
of my last couple minutes for rebuttal. 12:11:22

THE COURT: All right. 12:11:39

MR. JAMESON: Your Honor, may I proceed? 12:11:42

THE COURT: Yeah. 12:11:45

MR. JAMESON: I am going to start with somewhat of an 12:11:47
unusual place for the '856 patent, but it really provides 12:11:49
important context. 12:11:53

As you've heard, Centripetal contends that the 12:11:53
RuleGATE product practices every single patent being asserted in 12:11:58
this case. And if you look at the bottom left-hand corner of 12:12:02
this slide, you see that they say RuleGATE practices the '856 12:12:05
patent. And you've seen this slide before, and this shows where 12:12:09
RuleGATE is. And it's a, it's a real-time threat detector that 12:12:14
sits on the wire in front of firewalls and the network. And the 12:12:22
reason why I show that to you is because there is a complete 12:12:27
disconnect between what this claim covers and what they are 12:12:32
accusing. And with that, can we now go to slide 77? 12:12:36

Your Honor, they're accusing what Dr. Almeroth 12:12:44

referred to in his technology tutorial as an allow-and-detect 12:12:47
technology, or what I believe you, I believe, called 12:12:53
after-the-fact technology, where network threats have gotten 12:12:55
into the network and you start to analyze them to see if they 12:12:58
are malicious. And that's what they're accusing against a 12:13:02
claim. And Your Honor, I said in my opening, the language in 12:13:11
the claim is critically important. And we've got to understand 12:13:14
what this claim is about, and it begins at claim element A. 12:13:18
It's a packet filtering system. So we're talking about 12:13:23
filtering packets. And there's multiple steps that you do in 12:13:26
this packet filtering system. You identify packets that 12:13:31
comprise the unencrypted data, you identify packets that 12:13:36
comprise the encrypted data, and once you've identified that, 12:13:39
you then determine certain packets that might be encrypted that 12:13:43
correspond to a threat, and then the next thing you do is you 12:13:50
filter those packets. And you filter not only the packets that 12:13:55
comprise the unencrypted data, but you also filter the 12:14:01
determined packets that comprise the encrypted data. And once 12:14:05
you have done the filtering of packets, you then route the 12:14:12
filtered packets to a proxy. This claim is all about filtering 12:14:15
packets. And you're doing that real-time in a network. And 12:14:22
Your Honor, they want you to believe that they basically 12:14:28
invented using unencrypted data to detect bad things in 12:14:32
encrypted data. And if that's actually what they invented, they 12:14:37
would have been able to convince the Patent Office basically 12:14:42

stopping at claim element E. But they didn't. Everything you 12:14:45
see in red was added during the course of prosecution. The 12:14:49
filtering the packets, the determine packets and the routing, 12:14:54
that was all added in order to get the claim issued. And that's 12:14:57
critically important to the non-infringement issues. 12:15:02

I'm sorry, Your Honor, you were still reading. Let 12:15:08
me... 12:15:10

THE COURT: No, go ahead. That's all right. 12:15:12

MR. JAMESON: Okay. And we asked the inventor on this 12:15:14
patent about what's this invention all about. And the first 12:15:18
question was "Did you assume that Centripetal was the first 12:15:25
company to conceive of having an automated security system that 12:15:28
looked at the unencrypted fields of packet and for cybersecurity 12:15:31
threat detection purposes? 12:15:36

"Answer. I assumed we wouldn't be. I assumed the 12:15:37
uniqueness was using RuleGATE. That's their product." 12:15:40

And then the next question: "So you would be 12:15:45
surprised if Centripetal was the first company to have automated 12:15:47
computer systems for threat detection based on the unencrypted 12:15:50
portion of an encrypted computer network session; is that fair? 12:15:54

"Answer: Yes." The inventor would have been 12:15:58
surprised by that. 12:16:01

There are two reasons why we don't infringe this 12:16:04
claim. The first one is that we -- that StealthWatch does not 12:16:06
filter packets using the packet filtering rules as required by 12:16:12

the claim limitations F, F1 and F2. And Your Honor, this claim 12:16:17
language could not be any clearer. Beginning with claim element 12:16:25
F, you have to filter, in F1, packets comprising the portion of 12:16:30
unencrypted data, and you have to filter the determined packets 12:16:36
comprising the encrypted data. And we're filtering packets. 12:16:41
And we asked Dr. Cole, where is the packet filter located in the 12:16:47
system? And he gave an unequivocal answer. The packet filter 12:16:53
that's in StealthWatch Cloud with Cognitive Threat Analytics. 12:16:58
It's in StealthWatch. 12:17:03

And then we asked a follow-up question: "But the 12:17:08
original packet that came in that router or switch, they keep on 12:17:10
going and then the representations of those packets and NetFlow 12:17:14
records, they go up to StealthWatch. I think we've got 12:17:17
agreement on that, right? 12:17:21

"Answer: Yes, that is generally how it works." 12:17:23

The packets keep going to their intended destination, 12:17:29
and StealthWatch receives NetFlow records. 12:17:31

Briefly, Your Honor, this happened just a couple days 12:17:39
ago, one of the most straightforward questions I've ever asked 12:17:41
an expert. "Dr. Jaeger, does the filtering packets in claim 12:17:45
element F require filtering packets?" This led to the two and a 12:17:51
half minute answer, and the Court, spot-on, "The question only 12:17:55
refers to F1 through F2, it doesn't refer to G." 12:18:00

Rather than answering the question yes, it would be 12:18:05
the equivalent of saying is a red light red? Well, of course it 12:18:07

is. Does the claim language filtering packets require filtering 12:18:11
packets? He couldn't give me an answer. And the reason why he 12:18:15
didn't give me an answer is because Dr. Jaeger knew that 12:18:20
StealthWatch -- it's impossible for StealthWatch, the accused 12:18:23
device, to meet this claim element, can filter packets. That is 12:18:28
an impossibility. 12:18:32

And we got testimony taken from Mike Scheck of Cisco 12:18:36
on this very point. "And from the very beginning, with 12:18:39
StealthWatch in 2010, was StealthWatch ever a proactive tool? 12:18:44

"Answer: It was not. 12:18:46

"Question. Why not? 12:18:51

"Answer: Because the architecture has been the same 12:18:53
since 2010. It has always been a NetFlow consumption tool and 12:18:54
it has never been inline in a way to be, actually be 12:18:58
preventative. 12:19:03

"Question: Has it ever received packets? 12:19:04

"Answer: It has not. 12:19:06

"Question: Can StealthWatch filter packets? 12:19:08

"Answer: It cannot. 12:19:12

"Question: Can StealthWatch block packets as they 12:19:14
arrive into the network? 12:19:17

"Answer? They cannot." 12:19:19

Similar testimony was from Mr. Llewallyn. 12:19:22

And Your Honor, when it came to the -- 12:19:27

THE COURT: Didn't say much from Mr. Llewallyn. 12:19:30

MR. JAMESON: I'm sorry. I'll go back to it. It's in 12:19:33
the slides and I knew I was running out of time. I'm being told 12:19:36
that I'm good on time. 12:19:40

But what Mr. Llewallyn said in his first answer was, 12:19:42
"But as far as NetFlow goes, the packets are long gone and the 12:19:44
statistics about the packets are reported after the fact. 12:19:49

"Question: Would it be physically possible to block 12:19:52
those packets based on threat detection by ETA, CTA, 12:19:54
StealthWatch Flow Collector or any of that? 12:19:59

"Answer: No." 12:20:04

Mr. Llewallyn actually wrote the source code for 12:20:04
StealthWatch, and Your Honor -- 12:20:07

THE COURT: Okay. I've seen enough. 12:20:08

MR. JAMESON: -- with respect to this limitation, 12:20:11
Dr. Cole did not point to any source code. Instead, what he 12:20:12
pointed to -- and I know this was confusing in the record, but 12:20:19
it's so disconnected from the issue which is why it's 12:20:23
confusing -- he pointed to a thing called Cryptographic Audits. 12:20:26
And it is this diagram or this field in StealthWatch where 12:20:32
literally in a database you can filter on a field. It's got 12:20:40
nothing to do with filtering packets. And it's a human that 12:20:47
does this. It's a human filtering on a field. And this was 12:20:54
confusing and it was a complete disconnect, because this has 12:20:59
absolutely nothing to do with filtering packets. 12:21:03

More testimony from the inventor. "And the invention 12:21:10

of '856 patents, the actual threat detection again was on a 12:21:14
packet-by-packet basis inline, correct? 12:21:18

"That was my understanding." 12:21:21

There was nothing that was happening up in 12:21:24
StealthWatch that had anything to do with this patent. And he 12:21:26
said that in his first Q and A. 12:21:30

And so Your Honor, it's an impossibility for 12:21:35
StealthWatch to filter packets, and for that reason, we do not 12:21:41
meet claim elements F, F1 and F2. 12:21:44

And there can be no DoE because of all these 12:21:52
limitations were added during prosecution for the same reasons 12:21:56
that Mr. Gaudet already outlined with respect to the other 12:22:00
patents. 12:22:03

Turning to the last issue, and I know I think you -- I 12:22:11
suspect you feel like you've already heard enough about this, 12:22:16
but this is a critically important issue. And this is -- I 12:22:20
think it's a claim construction issue. 12:22:23

The accused proxy system, which they're saying is a 12:22:27
null interface, it is our view, it's our expert's view, that it 12:22:30
is not a proxy system that intervenes to prevent threats in the 12:22:35
communications between devices. And we went through this with 12:22:39
Dr. Cole, we went through this with Dr. Jaeger and we looked at 12:22:47
the specification of the '856 patent to gain insights on what is 12:22:50
the proxy system of the '856 patent. And Dr. Cole acknowledged 12:22:56
that packets are routed to a proxy system so that a proper 12:23:04

analysis can be done. A null interface doesn't do a proper 12:23:09
analysis, it drops packets. Dr. Jaeger agreed that a proxy 12:23:14
system could be used for further analysis or processing on 12:23:18
packets sent to it. We then provide you these cites from the 12:23:22
specification. Because what we see is in the specification, the 12:23:29
only proxy system described in the '856 patent is a system that 12:23:34
the combines a proxy device 112 with proxy device 114. 12:23:39

The other thing we learned is that there is no 12:23:43
disclosure of the proxy device dropping a packet in the '856 12:23:48
patent specification. Instead, what is disclosed as dropping 12:23:52
packets is this thing called the RuleGATE device. It's a 12:23:58
different device in the specification. 12:24:04

And then Your Honor, we provide the cites to 12:24:07
everything that the proxy system can do according to the 12:24:12
specification. It can set up a TCP session, it can receive 12:24:16
packets comprising data encrypted from a computer, it can 12:24:22
decrypt the data, it can generate one or more corresponding 12:24:27
packets comprising unencrypted data, and it can receive one or 12:24:31
more packets from the other proxy device. But the one thing 12:24:35
that is not disclosed is that the proxy system in the '856 12:24:39
patent specification drops packets. 12:24:45

And the only issue here, Your Honor, and this is what 12:24:52
Dr. Cole points to, is he says that the null interface is a 12:24:56
proxy system. And the document that he relies on, it describes 12:25:01
the null interface, and it states the null interface is not a 12:25:06

physical interface, it's a virtual interface, is always up, the 12:25:10 null interface, it never forwards or receives traffic, but 12:25:16 routes to -- but packets are routed there to be dropped. It's a 12:25:21 packet graveyard. And that's exactly what our expert testified 12:25:26 to, is that it is a packet graveyard. It is a black hole and 12:25:33 that it doesn't intervene in anything. And for that reason, it 12:25:38 cannot be the proxy system as construed by the Court in light of 12:25:43 the written description. For that reason, Your Honor, we don't 12:25:49 meet claim element G and we don't infringe the '856 patent. 12:25:54

Again, claim element G was added during prosecution, 12:26:02 so there can be no prosecution under -- no infringement under 12:26:07 the doctrine of equivalents. 12:26:10

And Your Honor that's all I have on the '856 patent. 12:26:14

THE COURT: All right. Any rebuttal? 12:26:20

MR. ANDRE: Yeah, Your Honor, just very briefly. 12:26:22

Counsel started off showing our product and said it 12:26:25 operates only inline. I'd like to show slide 147 of our slide 12:26:29 deck. 12:26:35

This is a blog that Cisco published on our technology. 12:26:35 And you can see on the right-hand side there is a RuleGATE 12:26:38 inline and there's a RuleGATE out-of-band or out of line. You 12:26:42 can see what that blue box, that orange diagonal mark going 12:26:46 through that, the RuleGATE, they keep saying it's inline only. 12:26:51 That's just not the case. That's obfuscation. 12:26:54

Second thing, they keep trying to parse, doing this 12:26:57

legal jiu jitsu to try to say that the claims mean something 12:27:01
that they don't. And they just, they keep cutting all the 12:27:05
different claims, taking pieces here and there. But in the end 12:27:09
they forget that that is a system we're talking about. They say 12:27:10
StealthWatch doesn't filter packets. Dr. Cole talked about 12:27:15
filtering many times throughout his testimony. They showed that 12:27:20
one clip every time. 12:27:24

If we go to the trial transcript, 955, Line 23 to 956 12:27:25
Line 2, and it says "And you provided evidence previously about 12:27:32
how the system filters through on domain names." This is right 12:27:41
out of the claim language. 12:27:44

He said, "We showed several pieces of evidence showing 12:27:44
domain names, even some testing that I performed that utilized 12:27:48
domain names." This is the badguys.com. That filtering of 12:27:48
those domain names was done at the routers and switches. 12:27:54
Packets are being filtered there." 12:27:57

In cross-examination, Mr. Jameson asked him, and this 12:28:00
is on trial transcript 1132, Lines 12 through 24. "Now, when I 12:28:05
crossed you earlier today you told me on multiple occasions that 12:28:08
the packet filter in the accused system is found in 12:28:08
StealthWatch. Do you recall that? 12:28:08

"Yes, I do. The main filtering is in StealthWatch. 12:28:20
This question was where did it begin. It begins by analyzing 12:28:22
the encrypted and unencrypted in the router and switches, but 12:28:25
then the main filtering is performed in StealthWatch. 12:28:28

"So just to be clear, with respect to the packet filtering element is in StealthWatch, right? 12:28:31 12:28:33

"The main packet filtering where we're analyzing the encrypted and unencrypted is in StealthWatch, because ETA is in the router and switch, the initial beginning of classifying encrypted and unencrypted begins in the routers and switches." 12:28:36 12:28:37 12:28:37 12:28:37

The initial filtering, Dr. Cole has stated on many occasions, I have multiple cites, initial filtering begins in the routers and switches. Representations of those packet are then sent to StealthWatch for further analysis. But to say that -- ignore the routers and switches as part of the system as Mr. Jameson just did, focusing only on StealthWatch, that's the whole crux of their defense, is just ignoring half of the infringing system. Or two thirds of it, actually. 12:28:42 12:28:51 12:28:54 12:28:57 12:29:02 12:29:06 12:29:09 12:29:14

So that's all I got on that, Your Honor. I think we said enough and we'll stay on time. 12:29:17 12:29:20

THE COURT: All right. Let's move on to the last patent. 12:29:22 12:29:28

MR. ANDRE: Last patent is the '176 patent, Your Honor. This is the correlation patent. 12:29:29 12:29:31

THE COURT: Right. 12:29:37

MR. ANDRE: Once again, Dr. Cole provided the expert testimony for us on this. He used multiple exhibits. This involves the switches and routers -- and if we go to the next slide -- and just StealthWatch. This does not involve the 12:29:38 12:29:42 12:29:45 12:29:48

Identity Services Engine. 12:29:51

Now the accused infringing system Dr. Cole talked 12:29:54
about is StealthWatch, and it gets logs from routers and 12:29:56
switches. It can be one router and switch, it can be multiple 12:30:01
routers and switches. The claims say a network device, meaning 12:30:05
one or more. 12:30:08

Dr. Cole talked about on many occasions he gave 12:30:10
examples of one, but can be one or more. All this really is is 12:30:13
logs that come from the switches and routers, go up to 12:30:17
StealthWatch where they're -- the analytics are performed there 12:30:21
to determine that there is threats. 12:30:24

So Dr. Cole's opinion was that the Catalyst 9000 12:30:28
switches and ASR -- and Aggregated Services Router and 12:30:32
Integrated Services Routers, embedded with ETA, working with 12:30:35
StealthWatch, integrated with ETA and CTA, infringes this 12:30:38
patent. The routers and switches connecting networks 12:30:41
together -- so any time you have a router and switch you have 12:30:44
different networks -- that identify packets from one network to 12:30:47
the other, and it generates log entries such as NetFlow or 12:30:50
Syslog or any kind of log entries you want to use, NetFlow is 12:30:53
the predominant one in Cisco's systems. They also looked at 12:30:55
Syslogs corresponding to the packets. The log entries are sent 12:30:59
to StealthWatch where the Cognitive Threat Analytics will 12:31:02
correlate the log entries from different networks, and based on 12:31:05
that correlation, a rule is generated and that is sent out to a 12:31:09

device in the first network. It's just provisioning the rule. And that's what this is about. This is about looking at traffic as it's coming across these network devices, routers and switches, taking log entries of that information, doing analysis, and trying to use intelligence to figure out if there's some threat, and if there is, it will generate a rule and send it to that device, a device on the network to enforce. 12:31:12 12:31:15 12:31:19 12:31:22 12:31:29 12:31:31 12:31:35

THE COURT: Is this rule generated before it is received? 12:31:38 12:31:43

MR. ANDRE: It will be generated in StealthWatch and then StealthWatch will send it out. So it'll be a rule that will be generated in StealthWatch, and then StealthWatch will send it to another device. 12:31:44 12:31:45 12:31:48 12:31:52

THE COURT: Before it reaches its destination? 12:31:53

MR. ANDRE: In this case -- no, not the logs. These are -- this is an instance where you don't have information about the packets coming through. So this is about looking at packets as they're coming through and it generating information about them. So this is a little bit different than trying and block them at the source. This is once you get information, you can generate rules and send it to the ISE, you can use these for exfiltration, you can do it for infiltration, future infiltrations. 12:31:57 12:32:00 12:32:04 12:32:09 12:32:12 12:32:15 12:32:19 12:32:24 12:32:28

THE COURT: The question is are the rules applied before it reaches the destination? 12:32:29 12:32:31

MR. ANDRE: Not, not the -- the log information, no, 12:32:35
Your Honor. The rules will be applied -- because what happened, 12:32:38
has happened, you have to correlate thousands of these packets. 12:32:41
You're getting packets from all these different routers and 12:32:46
switches. And so this is a correlation where you're looking at 12:32:49
potential threats. So the idea here is that when all this 12:32:53
information is being correlated, packets are still allowed to go 12:32:56
through unless they've been stopped for other reasons. Packets 12:32:59
are going through the system and they're trying to figure out 12:33:02
threat information based on this packet information they have 12:33:06
not seen before. There's no threat intelligence about it. So 12:33:09
they're trying to generate it. And they're doing it through a 12:33:11
correlation step. So the rule comes into effect after the 12:33:13
correlation is done. 12:33:17

THE COURT: Is the correlation done before it reaches 12:33:22
its final destination? 12:33:27

MR. ANDRE: No. The logs that are being -- that the 12:33:28
packets that are -- the logs that are going up, they would have 12:33:32
reached their final destination, Your Honor. 12:33:34

THE COURT: So this is reactive instead of proactive? 12:33:36

MR. ANDRE: It is, Your Honor. This is more looking 12:33:39
at reactive technology and trying to figure out if there's 12:33:41
something going on. What happens in many instances, and you 12:33:45
heard this in some of the tutorials both by Dr. Medvidovic and 12:33:49
Cisco's expert, that when an attack occurs, there is different 12:33:54

pivot points they come into, and they're coming into the 12:34:00 network, they may not have achieved their goal yet, but they're 12:34:02 trying to get into the network. So you try to stop before 12:34:06 there's a total breach and exfiltration of information or a 12:34:09 total infiltration of the network. But it is reactive in 12:34:11 nature, this patent is, because it has to do the correlation 12:34:17 before it actually generates a log -- before it generates a 12:34:19 rule. 12:34:22

THE COURT: All right. 12:34:26

MR. ANDRE: If we look at the testimony of Mr. 12:34:27 Llewallyn, we talked about this exactly. The example he showed 12:34:29 is exactly how it works. They're just not one router or switch, 12:34:38 it's usually several routers and switches. And it's very common 12:34:40 to get these logs from numerous routers and switches. So you're 12:34:43 getting log entries from numerous routers and switches going up 12:34:47 to StealthWatch, and that's what's going, the analytics in the 12:34:51 Cloud. And from the analytics, it's going to try to generate 12:34:53 threat intelligence. That's where the threat intelligence comes 12:34:57 from. 12:34:59

Now, Dr. Cole did test on this very aspect as well. 12:35:02 We go to PTX-408. He actually did set up his switch to specify 12:35:08 the ingress and egress. So he was looking at how the flow 12:35:17 monitor occurs going from one or the other or both. And you can 12:35:21 configure to get the logs from both. And that's from the first 12:35:25 and second network, essentially. But if you're getting it from 12:35:31

numerous switches and routers, you're getting it from the first and second network irregardless. 12:35:34 12:35:37

Now, if we go to the next slide, this is what we're talking about when we're talking about correlation. This is PTX-569. Says "StealthWatch Enterprise integrates with the Cloud based multi-stage machine learning analytics engine that correlates threat behaviors seen in the local environment with those seen globally. It employs a funnel of analytics techniques to detect advanced threats." 12:35:40 12:35:46 12:35:49 12:35:53 12:35:56 12:35:59 12:36:03

So what we're trying to do here is look at what's happening locally, getting this information and then correlating it to figure out what are the threats that are out there. These are unknown threats at this point. They're trying to identify them at this point. So that's what the correlation is all about. 12:36:05 12:36:08 12:36:11 12:36:14 12:36:17 12:36:20

We go to the next slide, this is StealthWatch with Cognitive Threat Analytics. This slide talks about StealthWatch integrates with Cognitive Threat Analytics. "This involves the addition of a new information panel on the CMS, enhances StealthWatch further by leveraging the CTA's Cloud-based analytics engine that correlates threat behavior seen in the enterprise with those seen globally." 12:36:22 12:36:27 12:36:30 12:36:33 12:36:37 12:36:42 12:36:45

So what this patent is about Your Honor, is looking all the information you can possibly get. You can get it from third parties, you can get it from the local traffic, you're 12:36:49 12:36:51 12:36:54

trying to use all this information. And this is a new way of 12:36:59
trying to detect threats. That's what this patent is about: 12:37:02
Using new methodologies, new analytics to detect threats through 12:37:05
correlation of local traffic and third-party stuff. It's the 12:37:10
local traffic doing those logs -- 12:37:15

THE COURT: So what's new about it is introducing the 12:37:17
third-party sources, is that what you're saying? 12:37:19

MR. ANDRE: No, it's correlating the logs, Your Honor. 12:37:22
Remember Your Honor, before ETA and before all this information, 12:37:26
the logs are just basically used for accounting purposes. Just 12:37:30
doing number counting. It wasn't done -- you aren't trying to 12:37:35
get threat intelligence out of log information. So what was new 12:37:38
here was there was this base of information of logs, there are 12:37:43
seven or eight different logging standards, logs that are done 12:37:51
for accounting purposes to see what the flow looks like, what 12:37:54
traffic looks like going across a switch or router. So what 12:37:58
this invention is about is using those logs to say let's enhance 12:38:01
those logs and get information from those logs that we can 12:38:06
actually maybe detect threats from. And you can correlate the 12:38:10
logs amongst themselves, that's the key here, you can also 12:38:13
correlate with other aspects as well. You can correlate any way 12:38:16
you want, but you have to correlate the logs together. That 12:38:19
local information is kind of the key here. 12:38:21

So that's what's new: Taking something that has been 12:38:24
done for years, which was the logging information, it's been 12:38:27

done for years, and then trying to figure out a way to make that 12:38:31 useful other than just accounting, other than just trying to 12:38:33 figure out what information is being -- the flow rates and the 12:38:37 number of packets going through per hour, per second or whatever 12:38:42 it is. So they took this information and now using it for 12:38:46 security. That was something brand new. 12:38:49

That was something that was introduced into the 12:38:52 StealthWatch system in 2017. They weren't doing it before then. 12:38:54 This is something that you look at now and you think, well, of 12:38:59 course they would do that. But they weren't doing that. No one 12:39:03 was doing it. 12:39:06

So if you go to the next page, and actually this is 12:39:08 where it was introduced. This is the StealthWatch System 6.10. 12:39:11 This is in 2017. It says "Cognitive Threat Analytics can now 12:39:16 leverage detections from analysis of WebFlow telemetry to 12:39:19 improve the efficiency of analyzing NetFlow activity from 12:39:23 StealthWatch. This is accomplished by system through 12:39:26 correlation of both telemetry types." These are the logs that 12:39:28 are going up. WebFlow is the Syslogs and other type of logs in 12:39:30 NetFlow correlating logs that are going into the system. So 12:39:36 this increased the detection of threats it says by approximately 12:39:40 10 percent. 12:39:44

Now, the only non-infringement position that Cisco 12:39:45 took in this case was by rewriting claim language. What their 12:39:54 expert said was a network device has to be the same network 12:40:04

device. The logs have to come from -- the packets have to come 12:40:08
from the same network device. And it has to be a single network 12:40:11
device. The same packets are being used as well, not all the 12:40:15
correlation of all different packets. That was the only 12:40:21
position that -- the non-infringement position that their expert 12:40:23
took. You have to completely take the claim language and 12:40:27
rewrite it to get there. 12:40:30

Mr. Llewallyn actually testified that In the case of 12:40:33
switch or routers, can generate both an ingress and egress 12:40:38
NetFlow record? And he said that's correct. It can be 12:40:41
configured to do that. The switch and router can be -- he 12:40:44
worded even if you were to rewrite the language as their expert 12:40:47
proposed, you can still get NetFlow records with ingress and 12:40:52
egress which are the two networks. 12:40:55

And then when asked has anything been done in the code 12:40:57
to deal with that problem, he said some customers do export 12:41:01
ingress and egress. So it's capable and some do it for their 12:41:04
own reasons. He's added the ability to configure the 12:41:08
StealthWatch to ignore one of those sides from the double 12:41:10
counts. So you still get it from the single network. 12:41:15

So even if you took the language as they rewrote it in 12:41:18
the claims, they would still infringe. You can't rewrite the 12:41:19
claim that way, because that is not how the system works and 12:41:25
that wasn't the testimony that was provided. 12:41:27

I'll save the rest of my time for rebuttal, Your 12:41:29

Honor. 12:41:32

THE COURT: All right. 12:41:33

MR. JAMESON: Your Honor, in response to your 12:41:39 questions, I think Mr. Andre has acknowledged a very important 12:41:42 point, which is he called this a reactive patent, and they're 12:41:46 trying to read a reactive patent on StealthWatch, which is a 12:41:53 reactive technology. And to your point, and I think this fact 12:42:01 is now crystal clear, that whenever we're involving 12:42:06 StealthWatch, we always know that the packets that have been 12:42:08 transmitted have received -- they have been received by their 12:42:12 intended destination. 12:42:16

What I would like to do again is start with the claim 12:42:20 language going to the next slide. And Your Honor, we're being 12:42:23 accused of rewriting the claim, but if we're rewriting the 12:42:36 claim, then Centripetal's expert, Dr. Cole, he rewrote the claim 12:42:38 as well, because his infringement theory is crystal clear: That 12:42:42 the ingress NetFlow record and the egress NetFlow record, they 12:42:48 have to be entering into or coming out from the same device, and 12:42:54 that the correlating step in C, that whatever's going to be -- 12:43:02 the correlating step, it has to be with respect to the ingress 12:43:08 record and the egress record that was originated by the same 12:43:17 device. And I'm going to get to Dr. Cole's testimony on that. 12:43:20

We give you the cites from the trial. And both on 12:43:30 direct and on cross he was asked the question "What's the 12:43:35 network device that you are accusing of infringement?" And he 12:43:38

says "It's the same switch or router. It receives packets." 12:43:42

THE COURT: Well, you haven't quoted the question and 12:43:46
answer here, you've -- 12:43:50

MR. JAMESON: Let's quote his question and answer. I 12:43:52
was going to do a summary. But let's get to what he says. 12:43:54

"Can you describe what we're looking at with both 12:44:00
these elements? 12:44:03

"Answer: Yes. So you have your router or switch and 12:44:04
you have network one and you're sending packets to network one. 12:44:10
It's initially received, and when it's received here it 12:44:13
generates logs. It would then generate logs. Then, with this 12:44:16
router or switch, takes the same packet and sends it out or is 12:44:21
transmitting it." 12:44:25

And then he goes on. "So essentially it's the same 12:44:29
router or switch that receives the packet and generates logs and 12:44:33
takes the packet, transmits it, and generates a second series of 12:44:38
logs. So the activity is performed by the same device." 12:44:41

We go on to the next paragraph. "But the activity of 12:44:50
receiving and transmitting and generating the logs is the same 12:44:54
activity. So in order to be concise, we're going to cover all 12:44:58
four of those together, because it's the same device." 12:45:02

And Dr. Almeroth methodically took this infringement 12:45:16
theory apart, and so now the theory is changing after the fact. 12:45:22

This diagram was put up in front of Dr. Cole and we 12:45:30
walked him through it. We've got the testimony here. It's the 12:45:34

same point as the last slide. You've got an accused switch or 12:45:38
router, packets go into it and go out of it, that's the ingress, 12:45:42
that's the egress, and a NetFlow record is created on the 12:45:46
ingress side, a egress NetFlow record on the egress side, and 12:45:51
then they would get sent up to StealthWatch. 12:45:56

THE COURT: There are no arrows here on this diagram. 12:46:00

MR. JAMESON: Right. The NetFlow record would go up 12:46:04
to StealthWatch. No, we all agree with that. 12:46:05

THE COURT: Well, that throws me off when you -- 12:46:09

MR. JAMESON: Sorry about that. We should have 12:46:13
extended the arrows. But the arrows absolutely would go up to 12:46:15
StealthWatch. And Centripetal certainly would agree with that, 12:46:19
otherwise they wouldn't have an infringement case. 12:46:22

And this is what he said. This is very important. 12:46:28
What are we correlating? And he says that "The correlating 12:46:29
and" -- 12:46:37

"Cognitive analytics is then going to do an analysis 12:46:37
on this data along with machine learning and threat 12:46:41
intelligence; is that fair? 12:46:44

"Answer: It performs a serious of correlation on, and 12:46:46
the important thing for me are the ingress and egress NetFlow 12:46:50
data. That's what you have to correlate according to claim 12:46:56
element C." 12:47:01

And then he says "There's nothing in the claim that's 12:47:03
exclusive to just those two, so there can be other data in there 12:47:07

as long as those two NetFlow records are being correlated." 12:47:13

His point was you may correlate with some other stuff 12:47:17
as well, but at a bare minimum you have to correlate those two 12:47:21
NetFlow records. And that was the next question. 12:47:25

"Okay. But just to be crystal clear about that point, 12:47:28
it's your opinion that the ingress NetFlow record and the egress 12:47:32
NetFlow record are actually correlated in Cognitive; is that 12:47:36
fair? 12:47:40

"Answer: In Cognitive Threat Analytics, correct." 12:47:42

That's what has to be correlated. 12:47:45

Here is how the system actually works. The person 12:47:49
that designed it and wrote the code. And we provide the trial 12:47:52
testimony. "StealthWatch was built to assume NetFlow records 12:47:58
are all ingress. When both ingress and egress NetFlow records 12:48:02
are sent to StealthWatch, that's considered an error 12:48:10
configuration." 12:48:14

We provided testimony and documents. Cisco tells 12:48:16
customers not to send both ingress and egress to StealthWatch. 12:48:20

Most importantly, we showed code that Mr. Llewallyn 12:48:27
wrote, Cisco wrote code to ignore egress NetFlow records to 12:48:31
rectify the error. Want it to reject any egress NetFlow records 12:48:37
that were sent to StealthWatch. 12:48:44

And then the final point, and this is actually 12:48:46
different, whatever NetFlow records are sent to StealthWatch, 12:48:48
they're not sent to Cognitive Threat Analytics for analysis. 12:48:54

And this document confirms that testimony. "For devices that use logical interfaces enabling both may cause flow collector to double report traffic stats in non-interfaced documents. We usually ask the customer to choose which dataset is most important." And this comes from the section of this exhibit, Troubleshooting NetFlow Configuration using StealthWatch. 12:49:01 12:49:09 12:49:14 12:49:18 12:49:21 12:49:26

And this is exactly what Dr. Almeroth testified as to why we don't infringe. Generating ingress and egress NetFlow records, that's considered an error. If StealthWatch were to receive both, it would result in an unnecessary double-counting, another error. 12:49:32 12:49:36 12:49:41 12:49:47 12:49:53

And finally, StealthWatch never passes the ingress and egress NetFlow records to Cognitive for correlation at all. 12:49:54 12:49:58

Dr. Cole cited three pieces of evidence, and Dr. Almeroth went through every single one of them, and actually one of them was just showed at slide 101 by Mr. Andre where it referenced WebFlow data. Well, that's not what the claim requires. The claim does not require correlating NetFlow data with WebFlow data that comes from a different device on the network. It has to come from the same device, per Dr. Cole. 12:50:07 12:50:10 12:50:15 12:50:20 12:50:24 12:50:28 12:50:32

Dr. Jaeger, who is their invalidity expert, he tried to rescue the case in rebuttal by making the claim construction argument that Mr. Andre just proffered. But the problem for Centripetal is that was not Dr. Cole's infringement theory. His infringement theory was crystal clear: We've got one device, 12:50:41 12:50:45 12:50:49 12:50:55 12:51:01

the NetFlow records come from the ingress and egress, they get 12:51:03
sent up to StealthWatch, but the evidence is crystal clear that 12:51:06
StealthWatch rejects and does not correlate those two records. 12:51:10
Therefore, we cannot infringe the correlation element. 12:51:15
Final point, and this gets to the last elements, D, D1 12:51:20
and D2, and this is the accused system does not generate and 12:51:27
provision rules. And Your Honor, go back up -- you know, I 12:51:32
won't go backwards in time, but if you go back up to the claim 12:51:38
element A2 -- well, actually I'm going to. Because this is 12:51:43
important. I'm going to go back to 101 real quick. 12:51:47
I'm going the wrong way. Can you take me to 101 12:51:50
please, Mr. Simons? 12:51:52
Your Honor, this is a system claim. And in A2, the 12:51:56
processor and the memory cause the system to do everything that 12:52:02
follows. The system. Identify, generate. Identify, generate, 12:52:08
correlate. The system responsive to the correlating, you 12:52:14
generate one or more rules and you provision with the one or 12:52:19
more rules, a device. It's the system that does that. 12:52:22
Can we go back to 113, please? 12:52:27
The problem with the infringement argument is that the 12:52:33
system does not generate and provision the rules. What they are 12:52:37
accusing of infringing claim elements D, D1 and D2, it's the 12:52:44
generation of an alarm or an alert. And an alarm or an alert is 12:52:51
not a rule. Those are sent to a system administrator to decide 12:52:56
what it might want to do by way of a diagnostic or further 12:53:01

preventive action. And that was the point Dr. Almeroth made. Alerts and alarms are not rules. As he stated, "Raising an alert there's suspicious behavior for a particular host is not a rule configured to identify the packets received as a required element of D2." 12:53:05 12:53:12 12:53:18 12:53:22 12:53:26

Instead, the way the accused system works is that when Cognitive or StealthWatch generates an alert or an alarm because of the possibility of suspicious behavior, you recall the testimony about Adam the Analyst. At that point in time, the alert or the alarm is sent to the StealthWatch Management Console, at which point in time Adam the Analyst can undertake an evaluation as to what to do. It can decide to take no action at all, or it can decide to limit access to the network. Quite frankly, Adam the Analyst may decide to create a new rule. But that's all manual by the human. And once that happened, Adam the Analyst would then send a message to ISE, at which point in time ISE could take action. And so there is human intervention all over what they are accusing of an infringement, and an alert or an alarm is not a rule per the Court's claim construction, and therefore these final elements D1 and D2 or not met for a second reason. 12:53:27 12:53:36 12:53:42 12:53:48 12:53:54 12:53:57 12:54:05 12:54:10 12:54:17 12:54:21 12:54:27 12:54:36 12:54:43 12:54:48 12:54:54 12:55:04

And whether it's this patent or any patent we're talking about, what I just told you about StealthWatch, there's always human intervention before anything gets sent back down to a network. So any claim that doesn't allow for human 12:55:10 12:55:15 12:55:20 12:55:26

intervention means it cannot read on StealthWatch. 12:55:30

And with that, Your Honor, that's the summary of our 12:55:33
non-infringement position. 12:55:37

MR. ANDRE: Your Honor, just a few minutes in 12:55:41
rebuttal? 12:55:43

THE COURT: Yes. 12:55:43

MR. ANDRE: Okay. So with respect to reactive versus 12:55:44
proactive, as we've shown you in numerous documents earlier 12:55:50
today, StealthWatch can be both proactive and reactive in 12:55:54
nature. That's the nature and what the product is. Says it can 12:55:57
be proactive to block threats and also be used forensic 12:55:59
reactively. That's undisputed, but that is -- you know, the 12:56:04
document speaks for themselves. 12:56:08

With respect to the actual claim language, if we go 12:56:09
back to slide 102 on our slide deck, this was an issue of 12:56:13
cross-examination where it says "the packets received by a 12:56:19
network device," everyone agrees in this case a network device 12:56:25
means one or more network devices, not the same one. The fact 12:56:30
that they refer back to the network devices with the antecedent 12:56:34
basis later means the one or more network devices. Dr. Cole 12:56:38
gave one example of using a single network device, and that's 12:56:43
where they landed, because they said that single network device 12:56:46
doesn't do both ingress and egress. That was the key to their 12:56:49
whole non-infringement case. It didn't do ingress and egress. 12:56:53
And then we showed Mr. Llewallyn's testimony. Because Dr. Cole 12:56:57

tested it, and I showed you his test where he used both ingress 12:57:02
and egress. 12:57:05

If we go to slide 103, the next slide, this was Mr. 12:57:06
Llewallyn's testimony. Again, can generate both ingress and 12:57:10
egress NetFlow records. That is correct. It can be configured 12:57:17
to do so. The switch or router can. The code is there. We 12:57:19
have a system and a code claim. The code is on the system to 12:57:23
generate both ingress and egress records. 12:57:28

Then they said he wrote code so where those ingress 12:57:32
and egress records would not be sent over for analysis. And 12:57:36
this was direct testimony. "Have you done something in the code 12:57:40
to deal with that problem? 12:57:42

"Some customers do export ingress and egress for their 12:57:43
own reasons." So people do it. But you can do it, it's in the 12:57:48
code. They do it. 12:57:51

"I've added the ability to configure the StealthWatch 12:57:53
Flow Collector to ignore it." So you can actually have the 12:57:55
coding in order as well. You can ignore the ingress and egress. 12:57:59
But the code is on the box. 12:58:03

When Dr. Cole did his test, he enabled both of them. 12:58:04
He enabled it on the StealthWatch, he enabled it on the Catalyst 12:58:07
switches. The fact that you're able to configure a system in a 12:58:11
different way doesn't mean the code's not there. 12:58:17

Your Honor, I think at that point we can -- 12:58:22

THE COURT: Well, where does this generate rules? 12:58:25

MR. ANDRE: Well, the rules are generated based on the 12:58:30
correlation, Your Honor. So the correlation is done up in 12:58:32
StealthWatch up in the analytics Cloud, the Cognitive Threat 12:58:36
Analytics. So all -- 12:58:41

THE COURT: StealthWatch generates the rules? 12:58:44

MR. ANDRE: That's correct, Your Honor. And then 12:58:46
StealthWatch provisions that rule to another device to enforce 12:58:49
it. We showed an example of the Identity Services Engine and 12:58:53
Dr. Cole's direct testimony. StealthWatch takes the -- 12:58:58

THE COURT: Let me look at that again. 12:59:02

MR. ANDRE: The testimony from Dr. Cole? 12:59:06

THE COURT: Well, where the rule is generated and 12:59:09
where it goes after it's generated. 12:59:15

MR. ANDRE: Well, the claim just requires generating 12:59:18
the rule and provisioning it to the device. 12:59:20

THE COURT: The claim says the rule will be generated 12:59:25
and sent somewhere? 12:59:28

MR. ANDRE: And sent somewhere, yes. It doesn't 12:59:30
require where it's being sent. But we have the -- I didn't show 12:59:32
it in my summary here, Your Honor. Let me see if I can find... 12:59:36

It's the exhibit, I think it's 1189. Doesn't look 12:59:41
right. It was like a 2,000-page document. It was one of those 12:59:55
long ones, Your Honor. 01:00:01

MR. JAMESON: Actually, Mr. Andre, I think what you're 01:00:17
looking for is the page before where Adam the Analyst takes 01:00:19

over. 01:00:22

MR. ANDRE: Sorry, Mr. Jameson, what exhibit are you 01:00:36
talking about? 01:00:38

MR. JAMESON: Well, it was the, it was the exhibit 01:00:39
that I -- it's my slide 116. PTX-1089. I was at 1239. And 01:00:40
this was the very document that I relied on that I think the 01:00:53
page before is what you all relied on, and then we just actually 01:00:56
provided exactly what happens. So you would want to pull up 01:00:59
1238. 01:01:04

MR. ANDRE: 1238? Let's see. 01:01:18

THE COURT: I remember seeing this exhibit, but I 01:01:20
don't remember... 01:01:21

MR. ANDRE: There it is, Your Honor. Let me just pull 01:01:22
up this figure here. 01:01:24

So this is the figure that Dr. Cole used in his direct 01:01:28
testimony and also used in his -- he showed source code for 01:01:32
this. So the suspicious behavior, zero, is notice for the host. 01:01:37
That's in StealthWatch. And then it applies the ANC policy, 01:01:42
quarantine. That's the rule that is being sent over to the ISE. 01:01:46
And then ISE can then say, okay, enforce this rule, whatever. 01:01:53
It doesn't matter for the purposes of this claim, it's just 01:01:58
sending the rule over to, provisioning it to another device. 01:02:02
What the ISE does with it, shows here, it goes down and puts 01:02:05
that rule onto the switches and does -- enforces the rule or the 01:02:09
policy. 01:02:14

This was the actual document that Dr. Cole relied upon, and his testimony is on page 1005 on that document. 01:02:15 01:02:20

THE COURT: Is this an exhibit? What is this? 01:02:33

MR. ANDRE: Yes, this is PTX-1089. Geoff, what page? 01:02:36

MR. JAMESON: It's PTX-1089 at 1238. And the next page explains actually what's going on, which is 1239, which is what I just used. 01:02:44 01:02:51 01:02:55

THE COURT: Okay. 01:02:57

MR. JAMESON: And those two pages together tell the story about that diagram and what's happening on 1239. 01:02:59 01:03:01

THE COURT: Okay. 01:03:08

MR. ANDRE: All right, Your Honor, I think we're up to our lunch break now. 01:03:11 01:03:15

THE COURT: Yeah, let's take our lunch break until 2:00. 01:03:16 01:03:18

MR. JAMESON: Thank you, Your Honor. 01:03:24

(Recess taken from 1:04 p.m. to 2:01 p.m.) 01:03:24

THE COURT: All right. Counsel ready for the invalidity arguments? 02:01:14 02:01:23

MR. GAUDET: Your Honor, we are. 02:01:25

THE COURT: All right. I think the first patent is '193. 02:01:27 02:01:30

MR. GAUDET: That is correct, Your Honor. And we're going actually start though on slide 4 of the book just for a moment, kind of get oriented. Mr. Simons, if you would pull 02:01:31 02:01:34 02:01:39

up 4? 02:01:46

Your Honor, Mr. Jameson touched on this this morning, 02:01:51 but this is, again, just to be very clear about our invalidity 02:01:54 methodology, it's completely based on the 01 Communique 02:01:58 approach, which is namely we do not think we infringe these 02:02:02 patents, and if you agree with them, then we wouldn't contest 02:02:05 that the patents are valid. For any patent that you agree we do 02:02:08 not infringe, we agree then we have not satisfied our burden to 02:02:11 invalidate. But any patent that you find we have infringed, 02:02:16 then based on that necessary claim scope, the patent would have 02:02:19 to be invalid. And that's exactly the methodology that the 02:02:22 Federal Circuit endorsed in the 01 Communique case. 02:02:26

Your Honor, with that introduction I'll turn to 02:02:31 slide 120 which gets us specifically into the '193 patent. 02:02:34

Your Honor, this is the exfiltration patent. Just to 02:02:41 get oriented, again we showed has the two-stage filtering 02:02:49 process. You see the origin and the destination in that first 02:02:53 stage, then you determine the particular type of data transfer 02:02:57 in the second stage. We will agree the prior art's not going to 02:03:00 show that. So you would have to disagree with that claim scope, 02:03:03 and if you do and find infringement, then the claim will be 02:03:06 invalid. And that's our point. That if to find infringement, 02:03:11 the claim will have to be invalid. 02:03:14

So the summary here about what was in the prior art, 02:03:17 that is kind of interesting, what we showed was the prior art 02:03:20

had the Cisco switches and routers like they're accusing today; 02:03:23
the prior art had the Identity Services Engine, that's the thing 02:03:27
they say creates the quarantine command -- 02:03:30

THE COURT: Excuse me. Let me call -- Brandan? I 02:03:34
probably pushed the wrong button here. 02:03:49

COURTROOM DEPUTY CLERK: Oh, I did that. I'm sorry. 02:03:52

THE COURT: I want to look at you, not at me. 02:03:53

All right. Go ahead. 02:03:59

MR. GAUDET: Okay. Thank you, Your Honor. 02:04:00

What I was saying on this slide is, what we looked at 02:04:01
in the prior art was what they had originally accused, which was 02:04:04
switches and routers that get a quarantine command from the 02:04:08
Identity Services Engine, and then we've got StealthWatch here, 02:04:13
because Dr. Mitzenmacher in his direct examination on 02:04:16
infringement, he referenced StealthWatch 24 times. They're now 02:04:20
saying that StealthWatch is not part of the infringement case at 02:04:27
all; that they're not accusing StealthWatch. And if that's the 02:04:29
case, then it means it's that much easier for this patent to be 02:04:33
invalid, because now all we've got are switches and routers that 02:04:38
get quarantine commands. And that is certainly prior art. 02:04:42

And Your Honor, this chart has a lot of words up here 02:04:47
and I'm not going to work through all these words right now. 02:04:53
This is to show you how, for each of the claim elements, we've 02:04:56
got a column with Centripetal's infringement theory, a column 02:05:01
for the corresponding functionality in the prior art, and then a 02:05:06

column for evidence that shows that. 02:05:11

The first few rows of the top row is just talking 02:05:12 about switches and routers. Then the next row that they receive 02:05:18 packets. This was where Dr. Mitzenmacher had talked about 02:05:24 StealthWatch. If he is, StealthWatch doesn't receive packets, 02:05:31 but just, today just like then, it would receive these 02:05:37 summaries. So if that's good enough today, that was good enough 02:05:40 back then, but now they're not even apparently accusing 02:05:43 StealthWatch. They're just talking about routers and switches 02:05:48 receiving packets. And they have always received packets. 02:05:50

Then the next set of limitations, Your Honor, again, 02:05:52 this filtering and what-not, they had accused StealthWatch, and 02:05:56 by the same token, StealthWatch back in the prior art we showed 02:06:01 could look for exfiltrations. Now they have withdrawn that and 02:06:05 now it's just the two latter bullets in the middle; namely, that 02:06:10 a human administrator can initiate a quarantine using the 02:06:13 Identity Services Engine and that a quarantine will stop packets 02:06:17 from going to a particular destination. That is unquestionably 02:06:23 in the prior art, Your Honor. 02:06:27

And then the last piece was essentially the same. 02:06:28

And so Your Honor, if you accept their infringement 02:06:33 theory of this very general reading of the patent, the patents 02:06:35 have to be invalid and none of the things they showed you, none 02:06:40 of the things about the recent press releases and all of the 02:06:44 great things about ETA had anything to do with their 02:06:47

infringement read, apparently, on this patent. 02:06:50

So here is kind of the history of the relevant prior 02:06:52 art here. We've got the sites. We've proved all this up, that 02:06:55 in April 2011, Cisco released the Identity Services Engine. 02:06:59 That's the thing that issues the quarantine. In March, 2012, 02:07:01 Cisco and Lancope, which used to own StealthWatch, integrated 02:07:08 the Identity Services Engine with StealthWatch. So StealthWatch 02:07:12 is a factor. Check that box. And then in April of 2012, Cisco 02:07:15 released Identity Services Engine 1.1, and that would actually 02:07:23 have that quarantine button on it. And also in April of 2012 02:07:26 Cisco actually marketed a system called the Cyber Threat Defense 02:07:31 Solution which was routers, Identity Services Engine and 02:07:33 StealthWatch. Which, ironically, is actually now apparently 02:07:39 more than their infringement read. All of that was before 02:07:44 March 12 of 2013. 02:07:47

Let me pause just a moment. This was collectively a 02:07:48 system, and so for purposes of anticipation, a system, the 02:07:53 system is the reference. The Cyber Threat Defense Solution 02:07:57 system. That's a single reference proved up by various 02:08:01 documents and various other evidence, okay? If you want to 02:08:04 consider each of the items separately, you could also consider 02:08:09 it through obviousness, and that would, obviously you would 02:08:12 combine these things because the document said combine these 02:08:16 things. So it's sort of a lay-down hand, if you will, of an 02:08:20 obviousness case where the documents literally say combine these 02:08:23

things. 02:08:28

Your Honor, we've presented a number of documents from 02:08:28 April, 2012, some before that. This is an example of an April, 02:08:31 2012 document. There were two other documents that were similar 02:08:36 in terms of the formatting but different documents, different 02:08:41 information, same date, April 9th, 2012 that explain this 02:08:46 system. And it has all the pieces here. It's got routers and 02:08:50 switches and Identity Services Engine and you name it. 02:08:54

So what was -- and this is a lot more complicated than 02:08:58 their infringement read. So what was it that their argument 02:09:03 was? What's their answer? Well, what we heard from Dr. Orso 02:09:06 was that back in the day, quarantines were different than they 02:09:11 are today; that the old quarantine was a "shutdown." It totally 02:09:15 shut down a device. That was the old quarantine. And that 02:09:21 today, today the new quarantine allows you to select which IP 02:09:25 addresses you can send to. So you don't totally shut things 02:09:32 down. Well, Your Honor, that's just not true. That's just not 02:09:35 what the evidence shows. This was the -- this is the graphic 02:09:40 user interface what the user would actually use in the prior 02:09:44 art, and Dr. Orso had to concede that, in the dropdown menu in 02:09:46 the middle left, quarantine is different than shutdown. 02:09:51

Quarantine then is exactly the same thing as 02:09:55 quarantine today. You select which IP addresses, in other 02:09:58 words, which addresses, which destinations, you can still send 02:10:02 packets to. It's typically like the help desk. A different 02:10:05

option is the shutdown that Dr. Orso was talking about. And we 02:10:10
also presented you with API or Application Program Interface 02:10:13
documents that showed you the same thing. We've just got the 02:10:18
trial cites here because we spent a lot time with Dr. Crovella 02:10:21
proving up exactly how prior art quarantines work, and also Dr. 02:10:24
Orso had to concede the same thing. There is no difference. 02:10:30

And this is now the testimony from Dr. Crovella making 02:10:33
the point, and it's a point about that previous image we just 02:10:37
looked at. It shows "Question: Dr. Crovella, what's on that 02:10:40
page." And he says "Certainly, very simply, it's showing an 02:10:44
operator could initiate a quarantine using the Identity Services 02:10:48
Engine in 2012 prior to the priority date of the patent." And 02:10:50
he goes on to say, you know, that's exactly what they're 02:10:55
accusing today. 02:10:59

And the next question is interesting as well. Said 02:11:00
"In both 2012 and today" -- this is the last question -- "does 02:11:03
that human analyst have to decide to do a quarantine like this. 02:11:08

"Yes. It's a manual process. It requires a human to 02:11:11
perform it. It was manual then, it's manual today." 02:11:14

There is nothing they have accused and no evidence 02:11:17
that would ever have an automated quarantine. It's always the 02:11:20
result of, I think we called them Adam the Analyst, the human 02:11:23
saying let's quarantine that device. It's all the same. 02:11:27

And so Your Honor, I just want to make a couple other 02:11:30
points, then I'm done on this patent. 02:11:33

First is that there was no second -- this issue of 02:11:35
secondary indicia of non-obviousness. In other words, even if 02:11:39
something seems obvious, if the patent holder can show there 02:11:44
must be this other evidence that proves it must not have been so 02:11:48
obvious, that's a very hard showing. They have to show specific 02:11:50
claim elements how evidence ties specifically to patent, and 02:11:54
Dr. Striegel didn't even try to do that. 02:11:58

The last issue is the other argument that Centripetal 02:12:01
made was that we didn't identify the level of skill in the art 02:12:06
for a person of ordinary skill in the art. And it's sort of 02:12:09
interesting. And we briefed this in response to their 52(c) 02:12:12
motion: Neither party did. It wasn't disputed. And if we had 02:12:17
to do it, so did they. I mean, the claims are read from the 02:12:20
perspective of one of ordinary skill in the art, so that would 02:12:24
be equally dispositive for them. But the reality is it's not 02:12:27
dispositive for either one of us, because the cases they've 02:12:31
cited don't say that you have to define the level of ordinary 02:12:34
skill in the art. If it's not disputed, it's not something that 02:12:37
you have to do. If it's a disputed issue and it would be 02:12:41
helpful you can certainly do it, but the cases they cited did 02:12:46
not say that this was some sort of dispositive error. In fact, 02:12:48
one them suggested you could just take the plaintiff's 02:12:52
definition if you're the only one who did it. And our experts 02:12:55
the only time this came into play, was to say would one of 02:12:58
ordinary skill in the art have known to combine the Identity 02:13:03

Services Engine, the router and StealthWatch. And of course 02:13:09
they would, because Cisco literally told you to. This is not a 02:13:13
hard obviousness combination. This is, as I said, sort of a 02:13:16
lay-down hand of an obvious combination. 02:13:21

Your Honor, that's everything I have on this. 02:13:25

THE COURT: All right. 02:13:26

MR. HANNAH: May I proceed? 02:13:31

THE COURT: Yes. 02:13:32

MR. HANNAH: Good afternoon, Your Honor. 02:13:32

The issue with Cisco's validity case is it has some 02:13:35
fundamental holes in the proof that they offer. Everyone knows 02:13:38
that validity requires clear and convincing evidence, and we do 02:13:44
not have any proof, much less clear and convincing proof, that 02:13:50
the prior art systems that they allegedly say existed in the 02:13:55
prior art meet the claim elements. 02:13:59

As Dr. Orso pointed out during his, in our rebuttal 02:14:02
case, there are wholesale elements that their expert didn't even 02:14:06
address. And we're going to get to those. Based on those, 02:14:13
based on not being able to even address the elements, the 02:14:17
validity case goes out the window. 02:14:21

So we turn to the next slide. This is the '193 02:14:23
patent. And it's valid over the Cisco's Cyber Threat Defense. 02:14:26
Now, we know that if we go to the next slide, the Catalyst 02:14:33
switches, we've shown a lot of evidence of this, was built from 02:14:38
the ground up. It's a new switch, a new product that came out, 02:14:41

and it was built from the ground up and integrated security. So for them to say that the old switches are the same as the new switches cuts directly against what their CEO said, what their documents say, and what all their manuals say. And so based on that fundamental premise that the old switches are the same thing as new switches, it just doesn't make sense. It definitely doesn't rise to clear and convincing evidence. 02:14:46 02:14:50 02:14:53 02:14:57 02:15:04 02:15:06 02:15:09

Let's look at the particular elements that are missing from the prior art and from Dr. Crovella's deficient opinion. You've seen this slide with Dr. Orso. During his direct testimony, Dr. Crovella never explained the quarantine in the prior art. He never did. When you look through the record, he never explained what the quarantine is. All he says is there is the word quarantine and that's it. They didn't show you anything during closing because it doesn't exist in the trial record. The only person that explained what the quarantine is was Dr. Orso in the rebuttal case. And he showed that the quarantining is different. In the prior art, the quarantining would completely shut down all communications from an endpoint completely. That is fundamentally different than how the brand new Catalyst switches and routers work today. Because the quarantining today will allow a particular type of data transfer based on the quarantine policy or block a particular type of data transfer based on that quarantine policy. That's not how it worked before these new Catalyst switches. And that's the 02:15:11 02:15:15 02:15:21 02:15:24 02:15:29 02:15:33 02:15:37 02:15:42 02:15:44 02:15:49 02:15:52 02:15:58 02:16:05 02:16:10 02:16:13 02:16:19 02:16:22 02:16:26

only evidence that we have in the record about what the 02:16:30
quarantining does in the prior art versus the quarantining here. 02:16:32
Because of that, there's no packet filtering rules as claimed. 02:16:37
As we discussed during the infringement earlier this morning, 02:16:41
the packet filtering rules allow particular type of data 02:16:45
transfer; that particular type of data transfer is to 02:16:50
unprotected resources or it'll block particular types of data 02:16:53
transfer to protected resources. There is nothing like that in 02:16:57
the prior art. Again, as I said, it completely shuts down the 02:17:01
endpoint. 02:17:08

The third and fourth bullet on this is that there is 02:17:09
just no discussion or proof of a first operator at all. Or no 02:17:12
discussion or proof of a second operator. We still didn't hear 02:17:16
it, even today. Even in closing arguments we didn't hear 02:17:19
anything about a first or second operator. And that's because, 02:17:23
again, it didn't exist. 02:17:25

The only -- and we're going get to this -- the only 02:17:28
operators that they mentioned when you search for the word 02:17:31
operator is this human operator. But that's not what's required 02:17:33
in the claims or in the patent specification. 02:17:36

Now I want to take to you DTX-711. DTX-711 is a 02:17:40
document that they used in their case. Dr. Crovella used this. 02:17:45
But all he did was show the word quarantine on the later pages. 02:17:50
That's all he did. He did not show the actual operation. 02:17:55

And if you go to the second page which Dr. Orso talked 02:18:00

about, it shows that you shut down the port of the endpoint. 02:18:03
That means no communications from that endpoint. You can't 02:18:08
allow data transfer to protected resources. You can't allow 02:18:13
data transfer to unprotected resources. You shut down the port 02:18:17
of that endpoint completely. That's what the quarantine did in 02:18:21
the prior art. 02:18:24

We turn to the operators. And we showed this slide 02:18:27
during Dr. Orso's testimony. And again, Dr. Orso testified, we 02:18:31
searched the transcript, he looked at it, he listened to the 02:18:37
testimony, and I asked him, during the rebuttal case, did he 02:18:40
identify an operator. He said no. This is an example of the 02:18:45
operator that was identified. He threw in the word a lot, he 02:18:48
said operator a lot, but every single time he's talking about 02:18:51
the operator is the human who is overseeing the computer 02:18:54
networks. And that's not -- that is clearly what is not 02:18:57
required in the claims. Because when you look at the -- when 02:19:01
you look at the specification and you go to figure 3, which we 02:19:04
showed -- the highlighting should be on "operator", it looks 02:19:09
like it got moved over -- but as you can see, the operator is 02:19:13
not a human. The operator is the allow or block that gets 02:19:17
applied when you analyze the traffic. And this is an important 02:19:23
point, because this is the exact same element that Cisco could 02:19:29
not prove during the IPRs. We showed this during the rebuttal 02:19:35
case. In the IPRs, Cisco put its best art forward. It tried to 02:19:40
invalidate the '193 patent. And the Board came back, the PTAB 02:19:47

board came back and said you have not proven with sufficient evidence that there is an operator in the prior art. It's the same for this case. They simply -- not only did they not show it in the art at all, they don't even mention it during their invalidity case. 02:19:54 02:19:57 02:20:01 02:20:06 02:20:10

So this is just additional evidence showing that they cannot show it in any of the prior art, in any of the prior art, and these are two elements of the claims that we just have no evidence for at all in the record. 02:20:11 02:20:15 02:20:19 02:20:23

And with that, Your Honor, we're missing at least four elements out of these claims. We're missing the responsive to a determination element from 18 and 19 that requires these packet filtering rules that can allow certain traffic but block other traffic. We do not have the first operator which is shown on this slide for both claims 18and 19. And if you go to the next slide, we're also missing the corresponding packet, the corresponding rules that will allow the traffic and the second operator that allows that traffic. We have simply no evidence of that in the record, and based on that, and the '193 is valid. 02:20:26 02:20:30 02:20:34 02:20:39 02:20:43 02:20:46 02:20:50 02:20:53 02:20:57 02:21:01

Unless Your Honor has any further questions, that's all I have for the '193. 02:21:08 02:21:11

THE COURT: Any rebuttal? 02:21:15

MR. GAUDET: Very briefly, Your Honor. 02:21:16

I think there were two issues he raises. With respect to the quarantine, we cited, gosh, it was about 30 -- it was a 02:21:18 02:21:20

good chunk of testimony from Dr. Crovella, and I want to call 02:21:27 out some specific lines where Dr. Crovella went through source 02:21:33 code about the Internet services engine. It was DTX-1433, 02:21:38 discussed at Lines 24, 57, 23, to 2460, 8. 02:21:43

He went through a number of documents in chapter and 02:21:50 verse showing how the quarantine worked and that it's exactly 02:21:53 like today, where the quarantine, you drop packets that have a 02:21:56 particular destination. And it's interesting, and Dr. Orso 02:22:00 confirmed the same thing on cross-examination, said this is one 02:22:04 of those examples where Mr. Hannah and I can debate it, but the 02:22:07 record says what it says. And we think it's pretty clear. 02:22:10

With respect to the operator issue, Your Honor, this 02:22:13 is the classic case of the patentee cannot say one thing to the 02:22:16 Patent Office and something different on infringement. Their 02:22:22 argument about what the operators were on infringement is that 02:22:25 anything that drops a packet is an operator. Anything that 02:22:29 allows the packet is the other operator, all right? We proved 02:22:33 convincingly that goes back decades; that of course a quarantine 02:22:37 can drop a packet or allow a packet. There's, according to 02:22:41 their infringement theory, there's no magic whatsoever. And of 02:22:44 course Dr. Crovella doesn't think that that is an operator, 02:22:47 because we don't -- that's not the way the claim should be 02:22:52 construed and we don't infringe. However, if you accept that 02:22:55 that is an operator, then we have demonstrated overwhelmingly 02:22:59 that of course that's exactly what quarantines do. It will drop 02:23:03

all traffic to a given destination and they will allow traffic 02:23:08
not going that destination regardless of the content. 02:23:11

Your Honor, that's all that I've got on that. 02:23:14

THE COURT: All right. The next patent is '806. 02:23:22

MR. GAUDET: '806, Your Honor, that one's me as well, 02:23:32
then I'll turn it over for a final time to Mr. Jameson after 02:23:33
this patent. 02:23:37

So Your Honor, the first slide on this one is 128. 02:23:42
And again, Your Honor, to orient you, the '806 patent is the 02:23:49
patent of the rule swapping, okay? And our prior art case is 02:23:57
essentially what's in this very straightforward testimony from 02:24:01
Peter Jones, all right? It gets more complicated when 02:24:05
Centripetal starts making their arguments, but this is it. 02:24:10
Centripetal is accusing the Catalyst 9000 ACL Hitless Update. 02:24:13
So the question, were these the first Catalyst switches to have 02:24:19
the Hitless ACL rule update? They were not. What other 02:24:22
Catalyst switches used that Hitless Update technique? Example 02:24:27
would be the Catalyst 6500. Specifically, the model called the 02:24:30
Supervisor 2T. And when was that product released? 2011. 02:24:35
Point blank. 02:24:41

THE COURT: I thought that Cisco had said that the 02:24:42
Catalyst 9000 was not an offshoot of the 6500 it was an offshoot 02:24:49
of the 3500? 02:25:01

MR. GAUDET: That is exactly right, Your Honor. And 02:25:03
this is going to put all of that in context, okay? 02:25:05

Mr. Jones worked on both of them. He's familiar with 02:25:08
both of them. And Your Honor, this is going to take a second, 02:25:12
but it's so important to get these facts nailed down, because 02:25:16
this answers the entirety, I believe, of Centripetal's argument, 02:25:19
okay? 02:25:25

This is kind of a funny-looking set of time lines, but 02:25:25
what this shows is the Catalyst 9000, that's using the IOS XE 02:25:28
all right? That family, its history is on the top. The 02:25:33
Catalyst 6500, its history is on the bottom. The stuff in green 02:25:38
is before Hitless ACL was used at all. The stuff in red is 02:25:43
after Hitless ACL was used at all. And so what you can see is, 02:25:50
on the top, the history of the Catalyst 9000 is 3850 and 3650, 02:25:55
when Peter Jones was working on it, and you move through here by 02:26:02
2016, 3650, 3850, 2019, Catalyst 9000 is released without 02:26:08
Hitless ACL Update. In 2018, for the first time, the Catalyst 02:26:14
9000 and IOS-XE have Hitless ACL Update. Separate history line. 02:26:20

Down below, the Catalyst 6500 history using the IOS, 02:26:28
in June or July of 2011, a very particular version released with 02:26:35
the IOS(50)SY was released with this same Hitless ACL Update 02:26:40
feature, but it did not make it into the Catalyst family because 02:26:49
it's a different source code line until 2018. Those are the 02:26:52
facts. 02:26:57

And Your Honor, with respect to the 2011, so we're at 02:26:58
6500, there are a number of documents that confirm it in 02:27:06
addition to Mr. Jones's testimony. The top document, this is a 02:27:09

2011 document, DTX-648, ACL Hitless Atomic Update. "This new 02:27:12
feature makes sure the production traffic is not affected by ACL 02:27:20
modification. The traffic will use the new ACL only when this 02:27:23
one is fully programmed in hardware." That is the essence of 02:27:27
Hitless ACL. 02:27:30

And the same thing, different document below it. It 02:27:32
allows updates to ACL without interrupting traffic. So that's 02:27:35
what is going on the 6500 side. 02:27:39

What's going on up in the Catalyst 9000 side? Well, 02:27:42
Your Honor, they used different hardware, different -- you know, 02:27:46
obviously, different software, and the timeline was just 02:27:53
different. And why does that matter? All right. An 02:27:56
extraordinarily confusing part of this trial -- and I 02:28:00
understand, and I wish there was a way to make it clearer -- was 02:28:03
Centripetal tried to argue that there are two different versions 02:28:08
of Hitless ACL, okay? They argued that the Catalyst 9000 had 02:28:12
some different version of Hitless ACL to the left of this red 02:28:18
bar, and that in 2018 what the Catalyst 9000 did was just get a 02:28:23
new and improved version of Hitless ACL. And the reason they 02:28:32
made that argument is that when Hitless ACL was introduced for 02:28:36
the first time in the Catalyst 9000, the documents referred to 02:28:41
the old way of doing things and they disparaged the old way of 02:28:44
doing things. But the old way of doing things was not Hitless 02:28:48
ACL, it was the version of the Catalyst 9000 and its predecessor 02:28:52
that had no Hitless ACL. And that's obviously not the prior art 02:28:56

we're relying on. So let me show you where the confusion came in. 02:29:00 02:29:03

This is the document we looked at yesterday. This is two pages, one after the other, okay, of the document that the plaintiff relied on talking about the Catalyst 9000. This is the document that came out describing that for the first time the Hitless ACL Update was going to be available, okay? And the right side is describing what that's going to be. It says "Hitless Atomic ACL Change Flow. For this new feature, Hitless Atomic ACL" -- exactly the same words, same description as the 2011 Catalyst 6500 -- "no packets will drop." Explains all about it. All about the things that it's going to do, all right? That is the same thing that was done in 2011. 02:29:05 02:29:06 02:29:11 02:29:14 02:29:21 02:29:28 02:29:31 02:29:37 02:29:43 02:29:47 02:29:51

Now, what Centripetal tried to argue is that the thing on the left which was just the old version of Catalyst 9000 without any Hitless ACL, was somehow Hitless ACL 1.0. It was some worse version that was the same thing that was back in the prior art. And that's just not what this document says. This document on the left never refers to the old system that Catalyst 9000 used as Hitless ACL. Because it wasn't. It simply didn't exist. That's what all of the trial evidence indicates. If it were, then somewhere on the left-hand page you would have found the phrase Hitless ACLS. 02:29:54 02:29:59 02:30:04 02:30:10 02:30:12 02:30:16 02:30:21 02:30:26 02:30:30 02:30:34

I've said a lot, why does this matter? Because all of the evidence in the case shows that the thing they were accusing 02:30:38 02:30:41

that was adopted in the Catalyst 9000 in 2018 is the same thing 02:30:45
that existed in a different family, a different device, back in 02:30:49
2011. 02:30:56

THE COURT: Why does it use the phrase "The current 02:30:58
Hitless" with something feature under Software Requirement? 02:31:03

MR. GAUDET: Absolutely, Your Honor. QoS is Quality 02:31:09
of Service. It's got nothing to do with Hitless ACL. I mean, 02:31:12
Hitless ACL, ACL are the rule changes. There are other Hitless 02:31:18
functionalities, but not Hitless ACL. ACLs are the Access 02:31:23
Control Lists. That's talking about -- so the phrase is talking 02:31:28
about the fact that there are only certain kinds of rules that 02:31:33
you can switch with Hitless ACL, and that list was similar to 02:31:40
that other thing was called Hitless QoS which is Quality of 02:31:46
Service. Hitless could -- again, if they meant that the thing 02:31:52
with respect to rule swaps was Hitless ACL, they would have said 02:31:55
it. It's just talking about something different, Your Honor. 02:31:59
That's the answer. 02:32:01

Your Honor, this now just makes all the 02:32:06
correspondences. It's similar to what we showed before. There 02:32:10
was one other argument that the plaintiff made. The other 02:32:14
argument that the plaintiff made was that we didn't say anything 02:32:16
about receiving packets and preprocessing. And again, to orient 02:32:19
you, this would be in the claim elements B down through at least 02:32:25
E. And this is there's a management device that's going to push 02:32:31
rules down to the routers or switches. And that management 02:32:35

device has to receive rules and then it does some work on the rules and it sends them down, okay? Now, they argued that we literally said nothing about that, and I'll show you what we said. This was Dr. Reddy, all right? And he was asked specifically about these limitations B through G. And the question. "Then if we go to the next column that corresponds to limitations B through G, you have a reference on the far right to rule sets created and updated. ACLs. Do you see that? That's what they're talking about? 02:32:40 02:32:43 02:32:47 02:32:51 02:32:56 02:33:01 02:33:05 02:33:08 02:33:11

"Yes, I do. 02:33:13

"And what does that correspond in the middle, in the middle column with respect to Centripetal's theory?" 02:33:14 02:33:16

Said, "Well, Centripetal alleges that the digital network architecture, that's DNA, allows these rules to be updated on the ACL, need to be updated on the Cisco switches, and corresponding L-A-M-I-R-A Management System in the Cisco products used to be called Prime Network Management System. And so it allowed similar features and similar functionality as being alleged in the middle. 02:33:19 02:33:24 02:33:29 02:33:32 02:33:38 02:33:41 02:33:45

"And the Prime Management Center that you'll be testifying about, what does that correspond to? 02:33:46 02:33:48

"Corresponds to DNA." 02:33:51

He says more. We put a document in. This is DTX-525. These were the release notes dated July of 2011 for this management system. And again, Your Honor, there's no magic 02:33:52 02:33:58 02:34:02

here: If the switch or device is switching rules, the rules have to come from somewhere, right? And the rules get received by this management device and they get set up and processed and pushed down to everything. That's not -- that process is not new. That's exactly what the Cisco Prime Network did. 02:34:06 02:34:10 02:34:15 02:34:19 02:34:24

And so middle of the question says, "Well, what is Cisco Prime Network Control System? 02:34:26 02:34:30

"Answer: This is a network management system that was available to manage Cisco products in the 2011 time frame." 02:34:32 02:34:34

We go to Bates Page 2 and Mr. Jameson asked, "Dr. Reddy, can you explain the significance of this bullet on Bates 2? 02:34:39 02:34:42 02:34:45

He says "This is showing the Prime Network to manage up to 5,000 Cisco Catalyst switches." Okay? 02:34:46 02:34:50

Last point, then I'm done, Your Honor. This is actually the last slide I think that you'll see from me. 02:34:53 02:34:55

Again, bring it back to the claims, Dr. Reddy. How does it impact? 02:35:00 02:35:03

And he says, B through G -- those were the very things that Centripetal's arguing that we ignored -- require processing of packets through a rule set. And this requires, as I've shown you in the infringement theory, Hitless Update and a network management system. And the accused product combination, it's a Digital network Architecture or Firepower Management Center. Similar functionality existed in the Prime Network Management 02:35:04 02:35:08 02:35:11 02:35:16 02:35:18 02:35:22 02:35:26

System that was available in 2011. 02:35:29

Your Honor, that's all that I have on this. 02:35:33

THE COURT: All right. 02:35:34

MR. HANNAH: Your Honor, may I proceed? 02:35:40

THE COURT: You may. 02:35:42

MR. HANNAH: I wrote it down, I think I wrote it down 02:35:45
three or four times, that the word confusing was used. 02:35:47
Confusing evidence is not clear and convincing evidence. All we 02:35:51
heard was attorney argument about these timelines and the 3500, 02:35:57
the 6500. None of that was presented during trial. The only 02:36:04
thing that was presented during trial was that the Hitless ACL 02:36:10
was updated and it was updated with the 2.0 version in the 02:36:17
Catalyst switches. 02:36:22

I'd just like to show the very -- the cover page of 02:36:25
PTX-1195. It doesn't say FED 2.0 Hitless ACL New Addition, it 02:36:29
says Update. They had a Hitless functionality and it changed. 02:36:39
The old Hitless functionality would overlap rules. And Dr. Orso 02:36:46
explained why. Because they wanted to apply the new rules as 02:36:52
soon as possible. The new version as shown on this document, 02:36:55
released in 2017, said we're dropping packets using the old 02:37:01
Hitless technology. We need to replace it and we're going to 02:37:07
replace it with the rule swap of the '806 patent. So the very 02:37:11
cover of this document cuts directly against the attorney 02:37:15
argument that was just made about there was never a Hitless 02:37:19
functionality ever at all on these Catalyst switches. 02:37:23

Turning to the slide deck, there's the same fundamental problem with the validity case the defendant have in that they just fail to prove a number of elements in the patents. I'm going to touch on it a little bit, but Dr. Orso explained it thoroughly that the original Hitless functionality did not swap rules and instead caused old rules and new rules to overlap. And we can show the slide deck just to get us oriented here. 02:37:28 02:37:34 02:37:39 02:37:42 02:37:51 02:37:56 02:38:01 02:38:10

A couple down, Geoff. Slide 115. 02:38:26

Rule swapping was not introduced into switches until 2017 with the FED 2.0. And I'm going to touch on that and I'm going to show you exactly, point out what Dr. Orso pointed out. 02:38:36 02:38:39 02:38:45

One key thing that we still haven't heard is that Cisco Prime, we don't know how it works. We didn't hear it from Dr. Reddy, we didn't see any documents about how it could receive rules. And even on closings we still don't know how Cisco Prime works. All we have is some vague statement that says it has similar functionality to DNA. Well, first, we proved that's wrong because DNA was built and released in 2017, and we showed documents of that. But that vague evidence is not clear and convincing evidence. They needed to prove that the Cisco Prime received the first and second rule set and did more than that; that it preprocessed those first and second rule sets just like the DNA Center does today. We showed ample evidence of that, about how it preprocessed rules, sends out policies. 02:38:50 02:38:53 02:39:01 02:39:06 02:39:12 02:39:17 02:39:22 02:39:26 02:39:33 02:39:36 02:39:39 02:39:43 02:39:49

Nothing of that nature worked at the Cisco Prime and we have no 02:39:52 evidence of that in the record. 02:39:56

So we go to the next slide. Dr. Orso explained this 02:40:00 very thoroughly in which he mapped the old ACL Hitless 02:40:05 functionality on the left and he actually showed the same 02:40:13 diagram that the defendant showed during their direct testimony 02:40:18 during Dr. Reddy's testimony. But Dr. Reddy failed to show the 02:40:22 comments. All they showed was the figure and said, oh, this 02:40:27 figure maps this figure. Well, if you actually look at it, the 02:40:32 bullet points don't match. Dr. Orso briefly touched that, but 02:40:34 that wasn't fundamental to his opinion. What was fundamental is 02:40:38 the explanation about how it worked. And Dr. Orso mapped that 02:40:41 exactly to this figure on the left. He showed how a new policy 02:40:45 is used temporarily. Why is that new policy used temporarily? 02:40:49 Because what they're trying to do is apply the new rules as soon 02:40:54 as possible. So they create this new, they create this new 02:40:56 policy and then they start writing these drop labels while the 02:41:01 old rules are still being implemented. While they're still 02:41:05 being used. And then they have to go through, use this label 02:41:09 policy. And if you remember, Dr. Orso pointed exactly to where 02:41:12 those labels were in the description of the 6500. How they used 02:41:16 these labels. And then they would delete this new policy, this 02:41:20 temporary policy, again shown exactly in the comments. What was 02:41:24 happening? Packets were dropping. It causes overlap. It 02:41:28 causes conflicts with the rules and they had to move on in 2017. 02:41:33

And if you look at everything on the right, there's no 02:41:38
use of a new policy, there's no overlap, there's no policy drop 02:41:41
label that's being used. You don't need that functionality if 02:41:46
you're just going to swap rules and you don't have to delete 02:41:49
this new policy -- amongst other changes. I mean, there's some 02:41:52
significant changes there -- and what does that result? Well, 02:41:55
first it results in infringement, but it also results in no 02:41:57
packets being dropped. 02:42:00

Now we go to the next slide. Dr. Orso performed a 02:42:05
similar analysis of trial testimony and he looked to see was 02:42:11
there any description of receiving rules. Literally looking for 02:42:15
those words to see if that was in there. Couldn't find it. If 02:42:20
you look for the word preprocess, again, it's completely absent 02:42:25
from the record. Saying that they're similar functionality is 02:42:29
not clear and convincing evidence about how a prior art system 02:42:34
works, especially when you don't even mention the words of the 02:42:37
claim. 02:42:40

So for these reasons, if you turn to the next slide, 02:42:41
there was no proof of receiving a first and second rule set, 02:42:45
there's no proof of preprocessing a rule set in the prior art, 02:42:49
because of that you can't perform anything after preprocessing. 02:42:54
And if you go to the last slide, there's just absolutely no 02:42:57
proof that the prior art swapped rule sets. The only evidence 02:43:02
in the record is that the prior art overlapped rule sets and 02:43:07
that the new system, the '806, the one that reads on the '806 02:43:11

patent, that's the system that swaps. 02:43:14

Unless Your Honor has any questions, that's all I have. 02:43:18 02:43:23

THE COURT: Any rebuttal? 02:43:23

MR. GAUDET: Your Honor, very briefly, and I will keep us ahead of schedule. 02:43:24 02:43:26

If we could, Mr. Simons, pull up Plaintiff's 1195, Page 1. 02:43:28 02:43:34

Your Honor, I want to start by addressing this same document. This is the document -- it's a 2017 document talking about the forthcoming change in the Catalyst 8000. And let's just look at the words, right? It's describing the Hitless ACL Update at the top. Mr. Hannah suggested that means it's an update to Hitless ACL functionality. No, that's the title of the functionality. You're updating the rules. You're updating the ACL. It's been called Hitless ACL Update since 2011. And to show you that, let's go to slide 130. ACL Hitless Atomic Update. It's not an update to Hitless ACL, it's that the software is talking about the Hitless way to update rules. 02:43:41 02:43:43 02:43:49 02:43:53 02:43:58 02:44:03 02:44:08 02:44:12 02:44:17 02:44:29 02:44:34

And let's go back to 1195. It's all over this document. What does this document do? Two lines down, it adds support for Hitless Atomic ACL Update feature. Because that feature didn't exist in the prior version of Catalyst or the prior version of FED that this is talking about, okay? 02:44:39 02:44:44 02:44:50 02:44:55 02:45:00

Likewise, if we go to Page 4 of this document, this is 02:45:05

where it's talking about the new feature, okay? Look at the first line under 2.2 Hitless Atomic ACL Change Flow. "For this new feature, Hitless Atomic ACL Change Flow." That's the new feature in Catalyst 9000, okay? It's the same thing that was in Catalyst 6500 in the prior art, and there is simply -- if what Mr. Hannah was saying were right, this document with refer to the old thing as Hitless. There is literally nothing that substantiates this claim that there was some earlier version of Hitless that was different. 02:45:10 02:45:14 02:45:20 02:45:25 02:45:30 02:45:35 02:45:38 02:45:42 02:45:46

And when I say confusion, you know, lawyer argument can create a lot of confusion. There's nothing on the face of these documents that supports the argument or that, when read on their face, would create confusion. That was my first point. 02:45:48 02:45:54 02:45:57 02:46:01

Second point, and this will be quicker. 02:46:04

With respect to Cisco Prime, that's the management center, Your Honor. Dr. Reddy told you everything you need to know. The only role of the management system according to Centripetal is it gets rules and it sends those rules down to the switch. And that's exactly what he showed Cisco Prime did and that's everything we have to do to match their infringement theory. 02:46:07 02:46:09 02:46:13 02:46:16 02:46:22 02:46:29 02:46:32

And Your Honor, with that, that's everything that I have. 02:46:32 02:46:33

THE COURT: All right. 02:46:37

Let's move to the '856 patent. The '205 patent was 02:46:50

not challenged for validity, right? 02:47:14

MR. JAMESON: That's correct, Your Honor. 02:47:17

We're slide 137, and I'm going to be brief. We're 02:47:19
going to stay ahead of schedule. 02:47:31

THE COURT: Okay. 02:47:43

MR. JAMESON: Your Honor, there is a consistent theme 02:47:44
with respect to invalidity, and Mr. Gaudet has laid out what 02:47:46
it's all about. Again, this is another patent that we do not 02:47:52
believe we infringe. But if you disagree with us, then Cisco 02:47:58
predecessor products would meet the elements at the same level 02:48:07
that Centripetal has proven up. 02:48:13

The priority date for the '856 patent is even easier 02:48:16
than the last couple you've looked at. It's December 23rd, 02:48:21
2015. So we're moving obviously a lot more forward in time. 02:48:25

We've got the same strategy, and this is going to be 02:48:32
laid out in our filing this afternoon where we work through 02:48:39
these lists with pinpoint cites. But we explain what they're 02:48:43
accusing on the left, what is the same functionality or features 02:48:51
in the prior art, and then we provide the evidence shown in 02:48:57
support on the right for each claim limitation. And I am 02:49:02
confident that I'm going hear from Mr. Andre that the '856 02:49:08
patent is all about CTA and ETA, and that's not what invalidity 02:49:16
is all about. We've got to look at what's the scope of the 02:49:21
claims that they're suggesting they have by way of claim scope, 02:49:26
and then we have to compare that to the features and 02:49:33

functionality in the prior art. 02:49:35

And if you look at the prior art column beginning just 02:49:39 at the second row, but I don't think there's anybody that's 02:49:47 going to challenge the issue about switches and routers. It is, 02:49:52 I think, beyond dispute that StealthWatch had been receiving 02:49:57 threat intelligence, including IP addresses and domain names, 02:50:01 going back since it's been in existence. And we provided some 02:50:04 testimony to that effect. I think where they're challenging us 02:50:09 is whether or not claim limitations C and D can be met with our 02:50:17 predecessor products, which is whether or not we were able to 02:50:23 identify unencrypted data and whether or not, using the 02:50:28 unencrypted data, we could then determine whether or not 02:50:33 encrypted data was bad or malicious. And on that point I want 02:50:38 to take a look at the next slide, which is DTX-364 at Bates 015. 02:50:45 And we talked a little bit with Dr. Jaeger about this yesterday, 02:50:54 and he was making the argument that port 443 doesn't necessarily 02:50:58 have anything to do with encrypted data. But if you look at the 02:51:08 specification that we compare it to on the right-hand side at 02:51:13 column 6, 36 through 45 and columns 18 at lines 9 through 18, 02:51:18 even the '856 patent acknowledges that "one or more ports (e.g. 02:51:26 port 443) indicated by transport layer headers in the packets 02:51:30 indicating the connection between hosts 106 and 142 will be 02:51:39 utilized to establish an encrypted communication session." 02:51:44 Because that's how port 443 is used. And then going back to the 02:51:47 left-hand side, that's also how the protocol HTTPS is used, as 02:51:55

that signifies an encrypted communication. 02:52:02

And so then we look at -- and this what StealthWatch shows, an alarm or an alert has been sent to the StealthWatch console, and it is identified that rule No. 1 on the right-hand side that there is an encrypted communication and potentially there's something suspicious with it. And it then sends an alarm to the StealthWatch Management Console. And the question becomes, well, how do you know that an encrypted communication might be bad or dangerous or malicious? Well, going back in time with old StealthWatch as they called it yesterday, old NetFlow, as apparently they would call it, that's exactly what old NetFlow records could be used for, is that you could use those NetFlow records to do an analysis of them to evaluate whether or not there was malicious traffic potentially in the network. 02:52:06 02:52:12 02:52:18 02:52:23 02:52:30 02:52:35 02:52:41 02:52:47 02:52:55 02:53:01 02:53:05 02:53:10 02:53:15 02:53:24

And the fact there are new -- the fact that there are two new fields in a NetFlow record today that are used by ETA, these patent claims don't say one word about the two new fields. If they did, we might have a different issue. But all they talk about is, at a broad level, whether or not you can use unencrypted information to identify encrypted information. 02:53:24 02:53:28 02:53:34 02:53:39 02:53:42 02:53:46

And that's what this very next slide shows. DTX-364. And this is, I want to focus on the text here. It says as you can see from the target host group column, the reason this rule fired is because the target of the communication was an IP 02:53:52 02:53:59 02:54:07 02:54:14

address in the Zeus botnet controller's host group. When StealthWatch did its analysis it was able to identify, because it had in its threat intelligence that this IP address was a dangerous IP address, and the reason it knew that was because the record that came up, certain of the fields in that record include the IP address. And that's actually, when you go to the right-hand side that's exactly what the '856 patent specification teaches as well as to how you are going to analyze potential encrypted information. It states it will "cause RuleGATE to determine, based on one or more network addresses included in the network layer headers, that the packets comprise data corresponding to the network threat indicators." 02:54:18 02:54:26 02:54:33 02:54:39 02:54:45 02:54:50 02:54:56 02:54:59 02:55:05 02:55:11 02:55:16 02:55:20

And as I understand it, that was the focus of Dr. Jaeger's attack on us. And I'm sure it may expand in closing, but that's what I heard yesterday. 02:55:24 02:55:26 02:55:34

And then going back to this, Your Honor, we have been crystal clear about this: StealthWatch is incapable of filtering packets. Can't do it. Because packets don't go to StealthWatch. And for that reason, we don't infringe. But if the filtering of packets in F1 and F2 means something different than filtering packets and it basically means filtering any results of anything that you can find on the StealthWatch console, well, we've been doing that forever. Because Adam the Analyst, using the StealthWatch console, he can drill down through hitting buttons to analyze information, filter 02:55:40 02:55:45 02:55:49 02:55:54 02:56:00 02:56:06 02:56:12 02:56:15 02:56:22 02:56:30

information any way -- not any way. Many duplicate ways. And 02:56:36 again, that's actually shown, Your Honor, just looking at the 02:56:41 top of the left-hand side of DTX-364, those little blue arrows, 02:56:46 those are buttons you can filter on to obtain additional 02:56:53 information about what's going on. And Your Honor, at some 02:56:57 level you might be going, well, that can't be what filtering 02:57:02 means. But that's exactly what Dr. Cole relied on. He relied 02:57:07 on the ability to filter within documents to satisfy these claim 02:57:13 limitations. And so this is the goose/gander rule. 02:57:18

And then finally -- I'm sorry, Your Honor, I keep on 02:57:26 hitting the wrong button. Let me back up. 02:57:31

With respect to the routing and the quarantining and 02:57:37 the proxy interface, actually Mr. Gaudet just took you through 02:57:40 this. There is no doubt that ISE in the prior art could 02:57:44 quarantine computers, and when it quarantined computers, that 02:57:49 packets would be blocked. And so if that's good enough current 02:57:58 day, then it was good enough back in the day. 02:58:04

The final point that I wanted to hit on, and it's the 02:58:13 lack of written description. Dr. Jaeger -- actually I think it 02:58:17 was Dr. Jaeger, criticized Cisco yesterday because the argument 02:58:23 was they haven't shown any documents that support their lack of 02:58:29 written description defense. And Your Honor, that was a new one 02:58:37 on me. Because the only document that can be used to support a 02:58:42 lack of written description defense is the written specification 02:58:47 itself. And it's either in there or it's not in there. And if 02:58:52

it's not in there, then there's your evidence to support your 02:58:59 written description defense. And what we know is they believe 02:59:03 that these claims, these packet filtering claims are broad 02:59:08 enough to encompass NetFlow and analyzing NetFlow records, and 02:59:14 that it's broad enough to encompass threat detection using 02:59:23 artificial intelligence and machine learning. And you can read 02:59:26 the specification from now for the rest of time, and neither one 02:59:32 of those concepts is anywhere in that specification. 02:59:36

We've got some other reasons here, but Your Honor, I 02:59:41 will stop for now. 02:59:44

THE COURT: All right. 02:59:48

MR. ANDRE: May I proceed, Your Honor? 02:59:53

THE COURT: Yes. 02:59:53

MR. ANDRE: I don't want to play cards with Mr. 02:59:55 Jameson, because he has that rule heads I win, tails you lose. 02:59:56 That's the way they have been trying this whole case. We can't 03:00:00 win regardless. If we win, we lose. That's just an unusual 03:00:03 strategy, but I guess it's a good one if you can pull it off. 03:00:07

Fact of the matter is, Your Honor, the issue with the 03:00:12 encrypted traffic was a big problem, and everyone knew it and 03:00:15 people were doing research on it. If you go to my favorite 03:00:18 press release ever, PTX-452, and it's also PTX-1135, this was 03:00:23 when Cisco announced the launch of this new networking. And it 03:00:29 says that "Cisco's Encrypted Traffic Analytics solves a network 03:00:33 security challenge previously thought to be unsolvable." That's 03:00:40

one of their executives who said that. Truth be known, why 03:00:43
their executives didn't show up at this trial, they would have 03:00:47
to defend all these statements they made. They can't come in 03:00:50
here and say to this Court we said all of that to our investors, 03:00:52
to the public, but we really didn't mean it. That's why they 03:00:57
weren't here. That's why they brought engineers to talk about 03:01:00
really complex, picayune details that really didn't matter at 03:01:03
the end of the day. 03:01:07

The press release talks about the Encrypted Traffic 03:01:09
Analytics being a, solving an unsolvable problem. It also talks 03:01:12
about the Catalyst switches being introduced, and a new family 03:01:17
of switches being built from the ground up. 03:01:20

If you look at the actual user manual for the Catalyst 03:01:22
switches, PTX-1417, it says "Before the introduction of the 03:01:25
Catalyst 9000 series, detecting attacks that hide inside 03:01:31
encrypted sessions required unwieldy and expensive measures." 03:01:35
They're talking about decrypting. "Cisco solved this problem by 03:01:38
delivering Encrypted Traffic Analytics on the Catalyst 9000 03:01:42
switch." Came out in 2017. That's Page 107 of that document. 03:01:46

The piece they keep missing here. They keep talking 03:01:58
about filtering packets for this patent. The switch and 03:02:01
routers, they start the filtering process. They have to filter. 03:02:04
That's the first step of filtering. They send representation up 03:02:09
to StealthWatch to do further filtering. When they talk about 03:02:13
the Encrypted Traffic Analytics with the new Cisco network and 03:02:17

StealthWatch on PTX-561, they once again state that "Cisco, with its experience in networking infrastructure market conducted extensive research and has introduced an innovative and revolutionary technology." That's how they're describing it. Innovative and revolutionary. They're coming into court the last six weeks saying we could do it all along. We have been doing it for years. There's noting innovative or revolutionary about this. 03:02:20 03:02:25 03:02:28 03:02:33 03:02:35 03:02:41 03:02:44 03:02:48

In their internal presentation on PTX-970 they say "Now available, Cisco's Encrypted Traffic Analytics. Industry's first network that can find threat in encrypted traffic without decryption." Without decryption is bold in their own document. That's what our patents are talking about, using the non-encrypted portion to look at the encrypted portion without decrypting it. 03:02:48 03:02:52 03:02:57 03:03:00 03:03:05 03:03:08 03:03:12

Their CEO trumpeted the success of the Catalyst 9000 switches saying "The key innovation on these 9000 switches was Encrypted Traffic Analytics." 03:03:14 03:03:19 03:03:23

And finally if we go back to the figure, we show the ETA solution with the 9K. We added this red text. The ETA was released in June of '17. Catalyst 9000 released in June of '17. Cognitive Threat Analytics was integrated with StealthWatch in '17. This is all well-after the time of the patent in 2015. 03:03:26 03:03:30 03:03:35 03:03:40 03:03:43

Now, the '856 patent is valid over the alleged prior art for a lot of reasons. One, and the easiest one is there's 03:03:58 03:04:02

no clear and convincing evidence to the contrary. The old 03:04:06 switches and routers did not have Encrypted Traffic Analytics 03:04:10 and they do not filter based on whether it was encrypted or not. 03:04:11 The ETA embedded on them was a game-changer. 03:04:16

The old StealthWatch did not have any concept of 03:04:19 determining network threat indicators in encrypted packets by 03:04:22 analyzing data from the unencrypted portions of the packet. The 03:04:26 concept just wasn't there. It was not even considered. The old 03:04:29 switches and routers and old StealthWatch did not filter 03:04:33 encrypted network traffic based on the unencrypted portions. 03:04:37 Didn't happen. They decrypted it. That's how they used to do 03:04:40 it. If you wanted to see what was in this encrypted traffic, 03:04:42 you decrypted it. ETA was not released until '17, CTA was not 03:04:45 integrated until '17 either. Those are the basic reasons. 03:04:49

Now they brought Dr. Schmidt on to talk about this, 03:04:54 and he used seven documents to try to show the old 03:04:57 StealthWatch -- and didn't show any of the switches or 03:05:01 routers -- the old StealthWatch can do. Five of the documents 03:05:03 DTX-311, DTX-343, DTX-364, DTX-380 and DTX-993, those five 03:05:08 documents, some of these documents are very long, 100 pages, 80 03:05:15 pages. These are very dense documents. The word "encryption" 03:05:18 does not appear. Just doesn't appear. It's just not there. 03:05:23 Encryption, crypt, cipher, decryption, nothing like that. The 03:05:28 concept was not even present, was not even is considered. 03:05:31

The two documents which the word encrypted appeared 03:05:34

on, they used seven documents total, had nothing to do with 03:05:38
trying to determine what was in the encrypted packets. 03:05:41

The old StealthWatch did NetFlow, but it didn't do 03:05:45
NetFlow that could distinguish the encrypted -- using the 03:05:50
unencrypted portion to try to figure out what was in the 03:05:55
encrypted portion. 03:05:58

The ETA flow records added in all these new fields, 03:05:59
Initial Data Packet being probably the most important one, but 03:06:02
also the Sequence of Packet Lengths and Times. That's what was 03:06:06
added into the ETA flow records. That was not there in the old 03:06:10
StealthWatch. IP addresses that will carry the day for you, and 03:06:16
it's not what is required by the claims. 03:06:21

If we look at what's actually missing from the prior 03:06:27
art and what Dr. Jaeger talked about, there was nothing in the 03:06:29
switches or routers that were identifying packets comprising 03:06:34
unencrypted data and encrypted. The concept just wasn't there. 03:06:37
It wasn't thought of. The packets, there was no distinguishing 03:06:42
between the two. They had to add that in to the switches and 03:06:45
routers. 03:06:47

Nothing in the old StealthWatch or the switches -- 03:06:49
they don't even talk about the old Identity Services Engine in 03:06:52
their allegations -- but none of that was trying to determine 03:06:59
what was in the encrypted part by looking at the unencrypted 03:07:04
part. That was that third element. 03:07:07

Filtering based on the domain name or any of these 03:07:11

fields were just not, once again, not considered. 03:07:16

And then routing based on what was determined by the 03:07:18
figured packets just did not exist. 03:07:23

One of the things that they keep bringing is the idea 03:07:27
that they could do this with Adam the Analyst. I'd like to meet 03:07:29
this Adam fellow, because he's got some magic in him. One of 03:07:33
the things that is essential about these claims, all the claims 03:07:38
in this case, there are system claims and they are CRM claims. 03:07:43
None of them are method claims. They seem to think that if it's 03:07:46
method claim you might have a problem with Adam the Analyst, but 03:07:51
with system claims, is the computer able to do it? If I turn 03:07:54
the computer on, it's going to do a lot of things. If I push 03:07:58
buttons, it's going to do a lot of things. It's the computer 03:08:01
doing it, it's not the analyst writing the rules, it's not the 03:08:03
analyst creating stuff. This is the analyst just pushing 03:08:07
buttons. So it makes no difference if Adam the Analyst is 03:08:10
pushing buttons or not, or if he could have used this model in 03:08:12
StealthWatch to come up with these possible elements. No art 03:08:16
out there suggested it. No one did it. 03:08:21

With respect to written description, Dr. Jaeger talked 03:08:24
about all the written support for the elements that they 03:08:28
identified in the '856 patent. Counsel just mentioned that one 03:08:32
thing is not stated in here is NetFlow. NetFlow is not 03:08:36
mentioned in the '856 patent. He asked a lot of our witnesses, 03:08:40
did you use NetFlow to determine this encrypted traffic? Is 03:08:44

that something you used. Keep in mind that previous slide, two 03:08:49 slides earlier when they add at the end the ETA flow records 03:08:55 into NetFlow, that wasn't until 2017. This patent was filed in 03:08:58 2015. In 2015, NetFlow was actually useless for determining the 03:09:04 difference between encrypted traffic and unencrypted traffic. 03:09:11 It didn't -- the concept did not exist. It wasn't until they 03:09:14 made this major renovation, wasn't until after they met with 03:09:16 Centripetal, they come up with this revelation of how to use 03:09:22 this type of information that NetFlow became useful. 03:09:24

That's all I have, Your Honor, unless you have any 03:09:32 questions. 03:09:34

THE COURT: No. 03:09:36

MR. JAMESON: Your Honor, just a few comments. 03:09:38

I will agree with Mr. Andre with respect to the last 03:09:42 two claim elements, that if you apply those claim elements the 03:09:44 right way, then the patents are valid. But with respect to the 03:09:47 elements that he also checked or used Xs on, I just showed you 03:09:51 documents that absolutely showed that the old technology was 03:09:57 using unencrypted information to identify malicious threats in 03:10:02 encrypted flows. And he put up a bunch of documents and said 03:10:07 the word description or decryption doesn't appear in any of 03:10:14 them, or encryption doesn't appear in any of them, but that's a 03:10:17 word game. Because the very document, one of the very five 03:10:20 documents that he relied on was the very document I put up 03:10:23 today, which was 364 at Bates 015, where we showed that the port 03:10:26

443 and the HTTPS is a reference to an encrypted flow just 03:10:33
described in the patent specification. 03:10:41

Mr. Andre, could we pull up slide 125, please? 03:10:48

Your Honor, I put up that marketing document in my 03:10:59
opening because -- well, I did it for a reason. I knew we were 03:11:01
going to dealing with this all day long. But you shouldn't have 03:11:07
to bring your CEO to a trial in a patent case to explain 03:11:11
marketing documents, and you shouldn't be criticized for 03:11:16
bringing some of the smartest engineers in the world to explain 03:11:19
the picayune details of the technology. Because this is a 03:11:27
patent case. But I am tired of seeing these documents. There 03:11:32
is, there is not a single word in PTX-515 that you can tie to a 03:11:39
claim element of any asserted patent in this case. Encrypted 03:11:48
Traffic Analytics, it might be accused as a product, but the two 03:11:55
new fields in Encrypted Traffic Analytics, the Initial Data 03:12:01
Packet field that Mr. McGrew invented, and the SPLT field that 03:12:05
Mr. McGrew and his team invented back in 2014 to '15, they don't 03:12:11
appear in any claim. They don't appear in the patent 03:12:17
specification. And the idea that the Catalyst 9000 is purely 03:12:21
about Encrypted Traffic Analytics and nothing else, I would just 03:12:27
simply ask you to read more of this document. But we can even 03:12:31
look at what we see here. Multi gigabit technology, 90W UPOE 03:12:36
Plus, onboard hosting. We can't go to the next page. There 03:12:42
were a lot of key innovations in the Catalyst 9000 switch that 03:12:46
Cisco is absolutely very, very proud of. But to go back to 03:12:52

where I started, which is whether we're talking invalidity or 03:13:07
infringement, we've got to look at the words of the claim. And 03:13:11
we can't genericize these claims and point to a document like 03:13:16
this one right here and say Encrypted Traffic Analytics, 03:13:23
therefore your invalidity defense is over because that was a new 03:13:27
product; or vice versa, look at Encrypted Traffic Analytics and 03:13:32
go we're accusing something that has to do with encrypted data, 03:13:36
therefore you infringe. That's just not, that's not good 03:13:41
enough. 03:13:44

That is really I have on this patent, and so absent 03:13:46
questions, we'll turn to the final patent, Your Honor. 03:13:52

THE COURT: All right. '176, the correlation patent. 03:13:59

MR. JAMESON: '176. And are you ready, Your Honor? 03:14:09

THE COURT: Yes. 03:14:21

MR. JAMESON: Once again, I guess we're going to be 03:14:26
playing the game of heads we win and tails they lose, because 03:14:27
it's our same theory. It's the one that 01 Communique 03:14:33
completely endorsed. But what we have shown here, and Dr. 03:14:37
Almeroth went through this in, quite frankly, painstaking detail 03:14:44
during the trial, is he took Centripetal's infringement theory 03:14:51
and he conceded on cross-examination on multiple occasions that, 03:14:56
you're right, I don't think, based on a proper claim scope, that 03:15:00
this patent is invalid. But if you're going to go after as 03:15:09
broad a level as what you are, then it's his opinion that the 03:15:15
claims are invalid. And starting at the top, he went through 03:15:20

documents and he showed that we've got switches and routers. 03:15:26
And then with respect to claim elements B1 through B4, he showed 03:15:30
that switches and routers have been receiving packets and 03:15:36
generating NetFlow records -- I mean, NetFlow was the standard, 03:15:41
Your Honor, back in 2004. And so by definition they have been 03:15:45
receiving packets and generating NetFlow records. 03:15:49

Where the disconnect came was, is claim element C. Is 03:15:54
the claim element why Dr. Almeroth didn't think we infringe. 03:16:00
Can old StealthWatch, can it correlate NetFlow records from a 03:16:06
ingress and an egress of the same switch or router? The answer 03:16:16
is it cannot. But if you can establish infringement by 03:16:21
correlating a NetFlow record with other information, other 03:16:30
threat intelligence, Syslog information, then StealthWatch has 03:16:36
been doing that since well-before the priority date. And Your 03:16:41
Honor, the priority date I didn't raise. The priority date is 03:16:46
February 10, 2015 for this patent. 03:16:52

THE COURT: I'm sorry, what is that? 03:16:58

MR. JAMESON: February 10, 2015. 03:17:01

THE COURT: Why do I have May 15th, 2015? Have I got 03:17:06
that wrong? 03:17:10

MR. JAMESON: Either I'm wrong with what I have 03:17:11
written down here or -- 03:17:13

THE COURT: I may have written them down wrong. 03:17:17

MR. JAMESON: Your Honor, at this point I could have 03:17:20
written it down wrong as well. But it's on the face of the 03:17:21

patent. I think that's the right date though. 03:17:26

THE COURT: What does it say? 03:17:33

MR. JAMESON: Oh, it was based on the, it's based on 03:17:36
the continuation application. That's where the priority date is 03:17:41
coming from. You've got the filing date of May 15. 03:17:46

Mr. Simons, pull that up just so it's clear what's 03:17:50
going on here. 03:17:53

The file date for the patent -- it's Row 22, if you 03:17:55
can highlight that? 03:17:57

And then that, this was a continuation of an 03:18:01
application that was filed February 10, 2015. So that's where 03:18:05
the priority date comes from. 03:18:09

THE COURT: Okay. 03:18:13

MR. JAMESON: And then Mr. Simons, if we could briefly 03:18:18
go back to slide 145? 03:18:21

And Your Honor, I've actually already hit on this 03:18:24
evidence, but this is the evidence that Dr. Almeroth relied on 03:18:26
where he showed processors and instructions and memory for 03:18:30
element A., and we got the testimony on the preceding slide, or 03:18:35
the cites to the testimony. 03:18:39

He relied on this document to show that you could 03:18:42
generate NetFlow records and identify packets based on summary 03:18:46
information, and that's DTX-311 at 010. That was claim element 03:18:53
B. 03:18:59

He then went back in time and he showed documents that 03:19:04

talk about the StealthWatch appliance and provides real-time data correlation, visualization and consolidated record reporting of combined NetFlow and identity analysis. And I've got to step back just because, you know, this is a prior art document, and even this document says provided real-time data correlation. Somehow or another that would be used against us because now NetFlow is real-time. I think it just means that it can do it quickly. But just an example of how -- 03:19:12 03:19:16 03:19:22 03:19:26 03:19:30 03:19:35 03:19:38 03:19:42

THE COURT: That's not what I think real-time means. 03:19:47

MR. JAMESON: Okay. Well, I don't think so either. 03:19:49

THE COURT: I don't think it means... 03:19:54

MR. JAMESON: Yeah. Okay. 03:19:55

And then finally just another a document, DTX-343 at 002 where he was correlating NetFlow with other things. And this was SLIC, SLIC threat intelligence feeds. And all that could be used to create alarms that would then be pushed down to a system administrator to then to take further action with respect to provisioning the network. 03:19:57 03:20:02 03:20:07 03:20:12 03:20:20 03:20:24

And then finally, Your Honor, I wanted to hit on lack of written description. And it's really the same point. It's really the same point all over again. The '176 patent doesn't talk about processing NetFlow records, doesn't talk about using artificial intelligence or machine learning, it doesn't talk about any of the concepts that are discussed here. And again, I'm not sure what more we're supposed to do when it comes to 03:20:28 03:20:35 03:20:40 03:20:46 03:20:50 03:20:56 03:20:59

written description other than to show the absence of disclosure in the patent. 03:21:03 03:21:10

With that, Your Honor, I will turn it over to Mr. Andre, absent questions. 03:21:11 03:21:13

THE COURT: All right. Mr. Andre? 03:21:17

MR. ANDRE: Your Honor, the accused systems here involve StealthWatch, routers and switches that provide logs to StealthWatch. 03:21:20 03:21:25 03:21:32

And you can go to the next slide, Geoff, please. 03:21:33

Now, what happens up in StealthWatch is kind of the key aspect here. Logs go up to StealthWatch, whether it be through NetFlow or Cisco logs, any kind of logs, whatever it is, and they go up -- 03:21:37 03:21:41 03:21:48 03:21:51

THE COURT: Is this the one that can be of any, of hundreds of sources? 03:21:52 03:21:56

MR. ANDRE: It can be, Your Honor. It can be logs from anywhere. They are -- the logs can come from, if you have one switch and router on the network, it will come from the one switch or router; if you have 10, it will come from 10. 03:22:00 03:22:01 03:22:08 03:22:13

The key issues for this patent with regards to validity is what's going on inside StealthWatch. It's just not putting those logs into a database and keeping them. It's doing something with them. It's doing analytics. And it's doing it with Cognitive Threat Analytics. That was integrated with StealthWatch in June of 2017. And it didn't begin correlation 03:22:16 03:22:21 03:22:24 03:22:27 03:22:31 03:22:35

of logs in the switches and routers until April, 2018. So they 03:22:39
say they have this technology earlier, but they didn't have 03:22:44
Cognitive Threat Analytics in StealthWatch. They didn't have 03:22:49
the correlation of logs in Cognitive Threat Analytics until June 03:22:51
of 2017, April 2018. 03:22:57

Now, could they send logs up to StealthWatch? Yeah. 03:23:00
Put it in a database and register those log. They didn't do 03:23:04
anything with them. Certainly didn't do what is required in the 03:23:09
patent where you correlate those logs to try and figure out if 03:23:12
some bad stuff's about to happen. So when you have the 03:23:15
responsive to correlation by the packets, you generate a rule 03:23:20
based on that, and you provision that rule to a device in that 03:23:24
first network, that just is not even a concept that was thought 03:23:28
of prior to the filing dates of this patent. 03:23:31

Now, there's many reasons why Cisco did not meet their 03:23:38
burden of clear and convincing evidence. The first one -- and 03:23:43
this was just a unusual thing to have someone say -- Dr. 03:23:48
Almeroth, their invalidity expert, said testified using the 03:23:51
proper claim construction the claims are valid. That's just 03:23:55
something that I don't know how that gets past the clear and 03:23:58
convincing evidence standard. The Cognitive Threat Analytics 03:24:02
wasn't integrated in StealthWatch until 2017. The old 03:24:03
StealthWatch did not perform the claimed correlation based on 03:24:07
log entries and the claims responsive to the correlation of 03:24:11
generating the rule and provisioning the rule. 03:24:15

Now, one of the things we talked about is the claims 03:24:17
don't require that all logs come from the same device. That's 03:24:20
just an issue -- it's a red herring. It can come from the same 03:24:24
device. It's not required. It can come from one or more. 03:24:28

When we talked to Mr. Llewallyn I asked him when 03:24:32
Cognitive Threat Analytics was it integrated with StealthWatch, 03:24:36
when did it happen, he says in 2017. Then version 6.1 -- 03:24:40
6.10.3. That's his trial testimony. So the Cognitive Threat 03:24:44
Analytics was not even in StealthWatch until 2017, two years 03:24:48
after the patent was filed. The priority date. So without the 03:24:53
Cognitive Threat Analytics, you get no correlation. And that's 03:24:59
the whole crux of the patent. 03:25:03

I mentioned Dr. Almeroth's testimony. And it was very 03:25:06
unusual testimony, to be quite candid. If you applied the same 03:25:11
interpretation you applied for infringement for the invalidity, 03:25:14
the claim would be valid, right? He says that's correct. And 03:25:15
that's their heads I win, tails you lose thing. But he said I'm 03:25:20
not offering opinions on what I believe is a proper claim scope. 03:25:24
I have never heard an expert say that. And I think that's 03:25:27
something that you can just take and you can't discount it by 03:25:30
saying we're doing it in the alternative. He's a technical 03:25:34
expert. He's not a lawyer. Lawyers make alternative arguments 03:25:37
all the time. The technical expert should be giving, under 03:25:42
oath, sworn testimony what they believe to be correct. I've 03:25:44
never had an expert say I'm giving an opinion I think is wrong. 03:25:48

So I think that is enough to take care of the clear and 03:25:51
convincing evidence standard. 03:25:54

When you look at the actual claim language and you see 03:25:57
what we're challenging here as not being in the prior art. The 03:26:02
packets that are received by the network device in the first 03:26:07
network and logs going up, we didn't challenge that. That is in 03:26:10
the prior art. Logs going up have been going up forever. The 03:26:14
correlating based on those logs, that's new. There's nothing 03:26:19
that shows correlating. Those logs were merely accounting 03:26:24
procedures only. They went to a database for accounting 03:26:28
purposes only. Then in 2018 Cisco started using them to figure 03:26:30
out threat detections. 03:26:36

In responsive to the correlation, the next element and 03:26:38
two sub elements, generate a rule configured to identify packets 03:26:42
received from that threat indication and you provision that rule 03:26:47
to a device, that was not even contemplated by Cisco's previous 03:26:51
systems. 03:26:57

With respect to the written description, Dr. Jaeger 03:27:09
went in, and I took some of the highlight clips. He showed for 03:27:12
each element that was challenged portions in the specification 03:27:16
that showed written description. Once again, they go back to 03:27:22
the tried-and-true method that we didn't refer to NetFlow in our 03:27:25
patents. As I said, NetFlow was not being used for correlation 03:27:31
at that time. NetFlow was not being used for ETA. NetFlow was 03:27:34
not being used for that type of information at that time. We 03:27:39

were using other type of log entries. You heard it from our 03:27:42
inventors and our technical people. We weren't using NetFlow, 03:27:46
we were using Syslog. We were using other logging information. 03:27:49
The fact that they figured out how to use NetFlow for their 03:27:52
logging information to detect threats, generate a rule and 03:27:57
provision that rule, well, I'm glad they came around to our way 03:28:00
of thinking and started infringing our patent. 03:28:04

That's all I have, Your Honor. 03:28:07

THE COURT: Any rebuttal? 03:28:10

MR. JAMESON: Very briefly, Your Honor. 03:28:12

We're playing ping-pong on what the law is, and Mr. 03:28:15
Andre is just wrong on the law under 01 Communique. He keeps 03:28:19
talking about the fact that Cognitive Threat Analytics was new. 03:28:23
It is. It was new. But Cognitive Threat Analytics is a machine 03:28:26
learning in the Cloud tool, and there's not a claim element in 03:28:31
this case that mentions machine learning in any way, shape or 03:28:35
form. That is a red herring. He is making the argument because 03:28:39
that we are accusing a new product, it is impossible to have an 03:28:46
invalidity case. And invalidity is not about a new product, a 03:28:51
new ETA, or a new Cognitive Threat Analytics. It's about 03:28:56
whether or not the same function or features or functionality 03:29:00
can be found in the art that comes within the scope of the 03:29:04
claims. 03:29:09

And can we pull up slide 133, Mr. Andre? Because 03:29:11
we've seen it a lot yesterday and again today, and I'm actually 03:29:19

going to just ask a question: Is this an exhibit or a 03:29:26
demonstrative? Because I have no idea what this is. Is this an 03:29:31
exhibit in the case, Mr. Andre? I'm just -- because I don't 03:29:36
know. 03:29:39

MR. ANDRE: Are you asking me? 03:29:45

MR. JAMESON: I'm asking whether this is an exhibit in 03:29:46
the case. I don't know what this is. Or is it a demonstrative? 03:29:48

MR. ANDRE: Well, it is a demonstrative based on the 03:29:53
actual, the StealthWatch that's in exhibit number -- what number 03:29:55
is that, guys? I forget the exhibit. These figures come from 03:30:03
an actual technical document from Cisco. But I put the red 03:30:07
lines in that said logs, and we put the red text in of when 03:30:12
these things were integrated. The actual StealthWatch itself, 03:30:16
the Cloud, the blue box is from technical documents, and those 03:30:18
little Catalyst switches are from the technical documents as 03:30:22
well. 03:30:26

THE COURT: What technical documents are they from? 03:30:26
In other words, this is not something that was copied straight 03:30:28
out of some technical document, this was created based on 03:30:34
something. What was it based on? The figures themselves come 03:30:43
from -- what's the -- was it 389? 03:30:49

MR. ANDRE: One second, Your Honor. I put all my 03:30:57
infringement stuff up. 03:31:02

Oh. 989, Your Honor. 989 has a flow -- 03:31:09

THE COURT: Is this plaintiff's or defendant's 989? 03:31:11

MR. ANDRE: PTX-989 at Page 33. So what we did, Your Honor, is show, it shows a single Catalyst switch going up to the StealthWatch, and what we did is we just added four additional Catalyst switches in to show it can be more than one. That's the original figure, it goes up to StealthWatch, the Catalyst switch. 03:31:15 03:31:20 03:31:25 03:31:30 03:31:33 03:31:36

THE COURT: That's slide 27? 03:31:37

MR. ANDRE: Slide 77, Your Honor. 03:31:40

THE COURT: Oh. 03:31:41

MR. ANDRE: So what we did was we took the, that figure for the StealthWatch and the Catalyst switch going up and we just showed what it would look like if you had multiple Catalyst switches, which we added. This is the ETA solution with the Catalyst 9K. We didn't show the ISE, it wasn't relevant to the infringement. 03:31:43 03:31:45 03:31:48 03:31:52 03:31:56 03:32:00

THE COURT: Okay. Okay. 03:32:01

MR. JAMESON: All right. So Your Honor, I would just -- obviously am now going to make an observation because they have relied on it a lot yesterday and today. All the red logs is not shown in the exhibit that they pulled it from. They created a bunch of additional switches, they added some red language and boxes to the right. So I mean this is, yeah, this is the ultimate demonstrative. But the final point that I'm going to make is whatever this -- actually I'm going to use Mr. Andre's word for one time in this trial: Whatever this cartoon 03:32:03 03:32:05 03:32:08 03:32:14 03:32:18 03:32:22 03:32:25 03:32:28 03:32:34

is showing, it is certainly not Dr. Cole's infringement theory. 03:32:39
And the record will speak for itself as to Dr. Cole's 03:32:42
infringement theory, which is that the NetFlow records have to 03:32:47
come from the same router or switch. 03:32:52

And with that, Your Honor, I don't have anything else 03:32:55
on the '176 patent. 03:32:57

THE COURT: All right. I think that counsel wanted to 03:33:02
also discuss non-monetary damages? You've got that on your 03:33:14
schedule. 03:33:22

MR. ANDRE: Well, Your Honor, we had 10 minutes each 03:33:30
reserved for just talking about non-monetary issues, relating to 03:33:32
damages or the like. 03:33:37

THE COURT: Do you think it's better to handle this 03:33:42
now or when we -- 03:33:44

MR. ANDRE: Well, Your Honor, what we want to talk 03:33:46
about is -- I think it's -- we can just tee it up now, and if it 03:33:49
comes in a little bit later, it's just ten minutes. What we 03:33:52
want to talk about in some degree is the willful infringement 03:33:56
issue, because -- 03:33:58

THE COURT: All right. 03:33:59

MR. ANDRE: -- it's a non-monetary issue, but it is 03:33:59
related to damages. Or could be. 03:34:02

THE COURT: All right. 03:34:06

MR. ANDRE: That's what we wanted to talk about. Then 03:34:06
we'll talk briefly about what we're looking at for equitable 03:34:08

relief as well. But we can do that later as well. 03:34:13

MR. JAMESON: I'm sorry, so what are we... 03:34:15
Judge, what would you like to hear from us on today? 03:34:17
I'm not sure if I'm completely following. 03:34:19

THE COURT: Well, you mentioned willfulness and 03:34:25
non-monetary relief. It seems to me that we ought to talk about 03:34:34
whatever relief, if any, the Court's going to grant when we talk 03:34:44
about damages. But I think if you want to talk about 03:34:50
willfulness now, that's appropriate. 03:34:58

MR. ANDRE: Okay, Your Honor. 03:35:00

MR. JAMESON: Your Honor, our preference would be to 03:35:02
wait, but we'll obviously do whatever -- 03:35:04
Actually, the reason why I want to wait, Mr. Andre, is 03:35:08
because I'm tired. 03:35:11

MR. ANDRE: Your Honor, I think we got a little time 03:35:13
left in the day, I would like to just go through the willfulness 03:35:15
issue and discuss this. 03:35:18

THE COURT: All right. I'll give you 10 minutes on 03:35:19
willfulness. 03:35:21

MR. ANDRE: Thank Your Honor. 03:35:22
As Your Honor has seen in this case, the timeline of 03:35:23
that Centripetal's interaction with Cisco, you notice that in 03:35:27
2015 there were multiple meetings. They were non-confidential. 03:35:32
No NDA was signed. And at that point Cisco's IP started hitting 03:35:35
our website. In 2016 throughout the entire year after an NDA 03:35:42

was signed, there were multiple meetings, multiple 03:35:46 presentations. Very highly proprietary, confidential 03:35:48 information was provided to Cisco. Seven months after the last 03:35:51 meeting and last presentation was given to them, they launched 03:35:56 their Network Intuitive. 03:35:59

One of the things that I want to show in the timeline 03:36:02 if we go a couple slides forward, the website hits correspond to 03:36:04 our meetings. One of the things we heard throughout this case 03:36:14 is that Cisco's people, some of the employees come in and saying 03:36:18 never heard of Centripetal, didn't want anything to do with 03:36:23 them, we saw their stuff, we didn't like it, but for a year and 03:36:26 a half they kept looking. They hit our website. And you look 03:36:29 at the next slide and you see how that corresponds to the 03:36:31 meetings they had through the year and a half. 03:36:34

We showed in this case that there was a 03:36:37 confidentiality agreement signed. That was PTX-99. And based 03:36:40 on that confidentiality agreement there was a presentation 03:36:44 given, and we showed the presentation as PTX-547 where 03:36:47 Centripetal's patented filtered algorithms were discussed, as 03:36:53 were the patents. 03:36:57

Go to the next slide. 03:37:00

We had Jonathan Rogers, the day after the meeting in 03:37:02 2016, they had the meeting on February 4th, 2016, on the 5th he 03:37:05 talked about, in a contemporaneous email, "The group seemed to 03:37:11 hone in on our filter technology and algorithms. The algorithms 03:37:15

are a significant networking technology with broad applications 03:37:18
we productize for security. There are also a few questions on 03:37:22
our patent." And we heard Cisco's witnesses come in and say 03:37:26
they didn't talk about algorithms, they didn't talk about 03:37:32
patents and there was nothing confidential. This email states 03:37:35
otherwise. 03:37:38

We also saw an email from one of the attendees, one of 03:37:40
the engineers who attended the meeting on the same day of the 03:37:44
meet on February 4, 2016, Mr. Keanini. And what he noted at the 03:37:47
end of his analysis was "What might be worth exploration is to 03:37:53
look at these algorithms" -- once again -- "they have and how 03:37:57
general purpose they may be for data synthesis - high 03:37:59
performance set theoretical functions. Again, knowing what 03:38:04
patent offices allow and not allow, I'd be very surprised if 03:38:08
they were able to make claims on the algorithms themselves. We 03:38:11
don't know until we study their claims." You heard them say 03:38:13
they didn't talk about patents, they didn't look at our patents, 03:38:17
we didn't talk about algorithms, but these contemporaneous 03:38:20
emails at the time say otherwise. 03:38:24

After the meeting they said they were no longer 03:38:30
interested in Centripetal's technology, but five months later 03:38:32
they invited Centripetal to be one of their partners at Cisco 03:38:38
Live. And they had a blog post, one of the Cisco's engineers 03:38:41
wrote about Centripetal, calling this really great technology. 03:38:46
He talked about how it could be deployed inline and out of band. 03:38:51

This is from Cisco's engineer, their blog, talking about our 03:38:54 technology, after we demonstrated the product to them again. 03:38:58

We then later in the year sent them a management 03:39:06 presentation. Once again, still under NDA, where we talk about 03:39:09 a robust patent portfolio, and we actually gave the architecture 03:39:14 road map for our systems. This is DTX-1270 -- PTX-1270. And 03:39:19 even talked about it's very sensitive. This is the kind of 03:39:33 information that we were giving Cisco because we thought we had 03:39:36 a potential to become partners with them, and it was under a 03:39:40 non-disclosure agreement. 03:39:44

After the communications ceased in 2016, in early 03:39:46 2017, we showed you during the opening statement testimony from 03:39:51 one of Cisco's engineers and asked "When did you specify the 03:39:56 requirements with respect to ETA? 03:40:02

He said "I believe it was 2017, early 2017." 03:40:03

And so "You submitted a requirement document in early 03:40:07 2017? 03:40:09

"Yes. 03:40:10

"And that is the point where development started on 03:40:11 ETA?" 03:40:13

And he said "Yes". 03:40:14

Cisco's brought in engineers saying they were doing 03:40:15 research on the encrypted traffic problem earlier than that. I 03:40:17 don't doubt they were. They didn't have the solution though 03:40:21 because what you see in the actual software functional and 03:40:27

design specification for ETA. This is their document, confidential document. They had the initial draft of the document in October of 2016 and they put in the requirement section in February of 2017. This is PTX-115. You'll see that all of the work that went into the software functional and design specification really started in February of 2017 and completed in June of 2017. 03:40:30 03:40:35 03:40:39 03:40:43 03:40:49 03:40:54 03:40:57

Now, there's been a lot made of whether they blatantly copied the information that Centripetal provided them in these meetings. I've never had a case where we find evidence that someone says, hey, I copied your stuff. It just doesn't happen. But here's what we know with respect to willful infringement: They knew about our patents, they knew about our technology, we educated them on how we solved the problems. That's what these algorithms are about. We educated their engineering team, several of their engineer teams about how we solved the problems because we had a non-disclosure agreement. How they used that to solve their problems, as Dr. Striegel said yesterday, it's highly likely, highly likely they used the information they learned to solve the problems they had with Encrypted Traffic Analytics, with rule swapping and others. 03:41:04 03:41:10 03:41:15 03:41:20 03:41:24 03:41:27 03:41:31 03:41:35 03:41:37 03:41:41 03:41:44 03:41:50 03:41:55 03:41:57

Your Honor, that's all I need to talk about with respect to willful infringement. Thank you. 03:42:02 03:42:04

THE COURT: All right. Does defendant care to respond? 03:42:08 03:42:11

MR. JAMESON: I don't want to respond, but I have no choice, Your Honor. 03:42:13 03:42:15

Dr. Striegel actually didn't say "highly likely", he said it was plausible. I have no idea what that means. 03:42:17 03:42:21

Can we pull up PTX-115, please? 03:42:24

Your Honor, Dr. McGrew gave extensive testimony about this. And Mr. Simons, if you will highlight this document right underneath the ETA software? 03:42:37 03:42:39 03:42:43

"This document describes the design of ETA on the Integrated Services Router, the 4K and the Aggregated Services Router, 1K." The record will speak crystal clear to this that ETA was first implemented in switches, and that happened before the February 4th, 2016 meeting with Centripetal, and once they had it implemented in switches they then transitioned to implement it in routers. 03:42:48 03:42:53 03:42:57 03:43:03 03:43:10 03:43:17 03:43:21

Can we pull up, I believe it was PTX-1270? 03:43:30

I'm sorry, is that DTX-1270? 03:43:38

I'm sorry, Your Honor, that's a different presentation. We can skip that one. 03:43:50 03:43:51

With respect to the February 2016 meeting, again, the record's going to be clear on this. There is a big difference in Centripetal saying we've got patented algorithms and we've got patents that cover our technology and actually affirmatively disclosing an algorithm that somehow or another Cisco would use. And the evidence is -- and quite frankly I don't know how you 03:43:55 03:44:04 03:44:07 03:44:11 03:44:17 03:44:21

would orally disclose an algorithm, because they're incredibly 03:44:25
math problems or equations. But the testimony in the record is 03:44:28
unequivocal on that, that the actual algorithms were not 03:44:34
disclosed. Centripetal made the point we have algorithms in our 03:44:38
technology which is why we can operate at five million rules, 03:44:43
which quite frankly, our response to that was it's an IPS on 03:44:47
steroids. That's not a criticism of their technology. Cisco 03:44:56
just didn't think that they needed it. 03:44:58

And Your Honor, I believe it was you, maybe it was 03:45:01
during openings, that you said this sounds like two parties that 03:45:04
dated but they didn't get married. And Your Honor, I think 03:45:09
that's exactly right. 03:45:15

And now I want to turn to slide 155, and I'm just 03:45:17
going hit on, very briefly, accusing a company of copying versus 03:45:26
accusing a company of infringement is two different things and 03:45:38
that's why they're saying willful infringement. And we still 03:45:41
don't know what is the disclosure that they made to us that 03:45:45
could be copied. It's vagaries. And we actually don't know 03:45:49
what it was that we copied and put into our technology. 03:45:55

What we do know is -- and you have seen all of this 03:46:00
evidence in the record -- that what got Centripetal worked up 03:46:04
about this case was when Cisco announced that we were releasing 03:46:08
or had released Encrypted Traffic Analytics and Mr. Rogers saw a 03:46:13
description of it in a white paper and he says "I hope you guys 03:46:18
are sitting down when you watch this, I knew it was flagrant but 03:46:23

not this fragrant" -- we're going to skip that, this was 03:46:26 testimony about kind of their internal investigation, but what I 03:46:32 wanted to show you, Your Honor, is what was in that white paper 03:46:36 was Cisco's disclosure of the Initial Data Packet. And down 03:46:42 here in the bottom right of slide 159, DTX-1179, Mr. Rogers 03:46:47 literally copied into his internal email correspondence the 03:46:53 Initial Data Packet. And that's what he was going "This is what 03:46:59 they have copied. This is blatant." It's the Initial Data 03:47:03 Packet. And that, Your Honor, is why we called Dr. McGrew to 03:47:07 trial: To establish unequivocally that in April 29, 2015, 03:47:13 well-before the February 2016 meeting, Dr. McGrew and team was 03:47:23 publishing to the world that they had come up with the Initial 03:47:32 Data Packet. And goes into excruciating detail as to what it 03:47:35 is. And we asked him all of this testimony, I will not go 03:47:40 through it now, but he says this document was dated 2015, and he 03:47:46 explained how they created the Initial Data Packet back in 2015. 03:47:52 And then this is the timeline that we have that explains all the 03:47:58 work that they did beginning in late 2014, and that we 03:48:01 actually -- he filed for a patent in May of 2015 in which the 03:48:06 Initial Data Packet was disclosed in the specification of the 03:48:12 patent. And we discussed that at trial. And I'm not going 03:48:16 through the rest of this because I think that's really where 03:48:23 their copying arguments were focused, is that somehow or another 03:48:28 we copied Encrypted Traffic Analytics. And the timeline, 03:48:34 slide 165, it shows what Cisco was doing beginning in 2014 all 03:48:38

the way up until the February 4th, 2016 meeting. And there was 03:48:47
disclosure after disclosure after disclosure of both Encrypted 03:48:55
Traffic Analytics, use of it in switches, use of the IDP, use of 03:48:57
the SPLT, and that there is no way from a timeline perspective 03:49:03
that that could have possibly have been copied from Centripetal. 03:49:08
And in fact, even Centripetal will admit that they have never 03:49:13
used an IDP or an SPLT, and it's not disclosed in any of their 03:49:18
patents. And those are the two fields that are in ETA. 03:49:22

The rest of the slides, Your Honor, we summarize the 03:49:29
testimony of the witnesses on the copying issue, and it's very 03:49:31
consistent. It's Jonathan Rogers versus his dad, his brother, 03:49:38
every Cisco witness that has testified in this case, and there's 03:49:45
no "there" there. 03:49:49

With that, Your Honor, I will say thank you for all 03:49:55
your time in connection with this trial. 03:49:58

MR. ANDRE: Your Honor, may I respond just for two 03:50:00
minutes? 03:50:02

THE COURT: Well, okay. 03:50:05

MR. ANDRE: All I have to say is Encrypted Traffic 03:50:08
Analytics is a whole lot more than two fields. It's a whole 03:50:10
process of doing analytics of that information. Adding two 03:50:13
fields are helpful, but that's not what ETA is. 03:50:18

They talk a lot about the fact they didn't invest in 03:50:21
the company. They talked to us for a year and a half and didn't 03:50:26
invest, and I believe they -- Mr. Jameson just talked about 03:50:29

dating and didn't get married. It's kind of like the old saying 03:50:32
I heard, why buy the cow when the milk was free. And that's 03:50:36
what it is for thee guys. They got our technology for free, 03:50:39
they didn't have to pay for it. That's all I have to say. 03:50:43
Thank you, Your Honor. 03:50:46

THE COURT: All right. Now I understand that where we 03:50:48
are on the data the Court requested is it would be delivered to 03:50:56
Dr. Becker I believe at the end of this week, which I'm not sure 03:51:04
what the end of this week means. 03:51:16

MR. JAMESON: I've got on update on that, Your Honor, 03:51:19
if you want me to give it to you. 03:51:20

THE COURT: Yes. 03:51:21

MR. JAMESON: I am being told that all of the -- all 03:51:22
of the data is being produced to Dr. Becker tomorrow, that data 03:51:28
will be produced to Centripetal when it is produced to Dr. 03:51:36
Becker, and that Dr. Becker intends to submit a report to the 03:51:41
Court, with your permission, by 4 p.m. next Thursday. He's got 03:51:46
to -- I mean, Your Honor, I'm not even going to try to explain 03:51:53
how complicated the data is. But that's what I'm being told. 03:51:59

THE COURT: All right. Well, both sides can submit a 03:52:08
report by 4:00 next Thursday. I have no way of judging how long 03:52:14
it's going to take to make a report on that data. That's not my 03:52:33
field. So if he thinks he needs that amount of time, then both 03:52:43
sides shall have that amount of time and they can submit 03:52:49
simultaneous reports as to exactly their read on what that data 03:52:52

is. But there was this evidence where somebody was saying that 03:53:01
their sales were increasing by double digits every quarter, I 03:53:15
believe, and double digits could be 10 percent or 99 percent, I 03:53:23
suppose. So I don't know what that means, No. 1. 03:53:32

There was testimony about there being seasonal 03:53:37
variations in sales of products, and so that's why I felt, to 03:53:40
get an accurate picture, we needed to look at the monthly sales 03:53:54
over a period of time and see if there was any trends there or 03:54:04
whatever. I don't know what else Dr. Becker's going to think of 03:54:08
the figures. 03:54:18

I think the plaintiff should submit a report from 03:54:29
their damages expert. I don't think it would be right for them 03:54:37
to bring in somebody new on this. Dr. Becker's doing it for the 03:54:41
defendant, so I think the plaintiff should use the financial 03:54:50
expert or one of the financial experts that they've already used 03:54:55
to make their report. 03:55:02

And the question is when should we schedule another 03:55:12
hearing? I've already -- I've got some other hearings 03:55:16
scheduled, although the only thing that I'm 100 percent sure of 03:55:36
infringement-wise is that this case has infringed on my 03:55:45
retirement. 03:55:50

But what do we have... Let's see, if we get the report 03:55:51
next Thursday... 03:56:06

COURTROOM DEPUTY CLERK: If we get the report next 03:56:10
Thursday we have July 1st in the afternoon. 03:56:20

THE COURT: Well, next Thursday -- wait a minute, next 03:56:22
Thursday would be the 18th? 03:56:26

COURTROOM DEPUTY CLERK: Next Thursday is the 18th. 03:56:32

THE COURT: All right. What do I have on the 25th? 03:56:35

COURTROOM DEPUTY CLERK: You have nothing on the 25th. 03:56:43

THE COURT: All right. 03:56:46

COURTROOM DEPUTY CLERK: Could do it at 11:00 on the 03:56:52
25th by Zoom. 03:56:54

THE COURT: Yes. 03:56:56

COURTROOM DEPUTY CLERK: June 25th at 11:00, counsel, 03:57:02
by Zoom? 03:57:06

MR. ANDRE: That's fine for plaintiff, Your Honor. 03:57:08

MR. JAMESON: The only question I have is are you 03:57:11
going to want the experts available on the 25th, and if so, I've 03:57:16
got -- if we can have until at least tomorrow to see if -- or 03:57:21
later today to see if Dr. Becker's available? 03:57:25

THE COURT: Well, I want to get it done that week, so 03:57:33
if he's not available that day, we would move it closer. 03:57:36

MR. JAMESON: That may actually be -- I have no idea. 03:57:43
I was just asking the question, because I've got no idea what 03:57:46
his availability is. 03:57:48

THE COURT: I know when I was practicing law, of 03:57:50
course my experts were usually physicians, and they never let 03:57:52
testifying interfere with a skiing trip or a golf trip. So I 03:57:58
know what the problems are in dealing with them. So we'll have 03:58:04

to verify the availability of the experts. 03:58:10

MR. JAMESON: We're checking as we speak. And if for some reason that doesn't work -- well, for whatever reason, if it's for good cause, we would notify the Court immediately either later today or tomorrow. 03:58:18 03:58:24 03:58:27 03:58:29

THE COURT: All right. 03:58:32

MR. ANDRE: Your Honor, the good thing about using this format, this the Zoom format is it works on the beaches and ski slopes just as well as anywhere else. 03:58:33 03:58:34 03:58:37

THE COURT: That's true. 03:58:41

MR. ANDRE: The experts are going to run out of excuses. 03:58:44 03:58:47

MR. JAMESON: That is true. I think you're absolutely right about that. 03:58:48 03:58:50

THE COURT: I hadn't thought of that. We could catch them right on the slopes, couldn't we? 03:58:51 03:58:54

MR. ANDRE: Yeah. Even lawyers have run out of excuses now. You can't use vacation as an excuse anymore for hearings. It's a new era. A new day. 03:58:57 03:59:00 03:59:03

THE COURT: Right. Right. 03:59:06

MR. JAMESON: And Your Honor, I'm going to ask just for a point of clarification because I think I understand, but I want to make sure the same rules of the road. We're going to turn the data over to the experts and they are going to create a report that basically explains what the data shows, and that's 03:59:07 03:59:08 03:59:11 03:59:15 03:59:19

going to be the sum and substance of their report, not a revised 03:59:24
damages opinion or something like that? Because that's a whole 03:59:28
new, that's a whole can of worms. 03:59:31

THE COURT: I agree with you. No, I don't think -- I 03:59:34
think they just want to say just as you said -- 03:59:35

MR. JAMESON: Okay. 03:59:44

THE COURT: -- how that data affects the opinion that 03:59:44
they have already given, if any. 03:59:48

MR. JAMESON: Okay. 03:59:50

THE COURT: What affect it would have. But I don't 03:59:52
think they should come up with a new damages figure. I think 03:59:54
the Court's going to have to do that if I award damages. And as 03:59:59
I say, the Federal Circuit has talked about how difficult that 04:00:10
is. But I think the Court's going to have to do that. I don't 04:00:15
think we can reinvent the wheel at this point in the case. 04:00:22

So between now and then we'll be working on the issues 04:00:32
of infringement and invalidity. I don't know if you want to be 04:00:52
further heard on the issue of willfulness or not. 04:01:05

MR. ANDRE: Your Honor, from plaintiff's point of 04:01:12
view, I think the record has been made and we have addressed it 04:01:13
here in closing. I think the only thing that we would want to 04:01:17
address down the road is, you know, on the subsequent closing 04:01:21
would be the damages issue -- 04:01:25

THE COURT: All right. 04:01:29

MR. ANDRE: -- and remedies. 04:01:30

THE COURT: All right? Does defendant agree with 04:01:32
that? 04:01:37

MR. JAMESON: Your Honor, I think a closing on damages 04:01:38
would be appropriate. I'm not sure what other remedies he's 04:01:40
talking about, but I do agree we ought to have a closing on 04:01:44
damages. 04:01:47

THE COURT: Yeah. Well, okay. 04:01:49

Well, I would say that the case certainly took a long 04:02:00
time, but it involved very complicated and I think important 04:02:06
technology. I just bought a self-driving car, and I thought 04:02:14
that I hope that the network which drives it will be secure. I 04:02:24
hope nobody is able to put malware into self-driving cars to 04:02:35
cause collisions. 04:02:46

MR. ANDRE: Especially as after-the-fact. 04:02:49

THE COURT: Right. Yeah. I would hope it would be 04:02:52
proactive. 04:02:57

MR. JAMESON: Your Honor, I was actually at a CLE 04:02:58
about a year ago, and the people that are in that industry said 04:03:00
that is the single biggest issue that they're dealing with, is 04:03:04
cybersecurity relating to self-driving cars. 04:03:08

THE COURT: Yeah. Well, I hope your guys' clients can 04:03:11
figure that out, or somebody can. 04:03:17

But anyway, I think there's justification for the case 04:03:22
taking as long as it did. I don't think it had anything to do 04:03:27
with the format. I think the format worked very well. If 04:03:32

anything, I think the Court's ability to evaluate the 04:03:36
credibility of the witnesses was probably improved by the 04:03:42
format, because I was not distracted by anything happening in 04:03:47
the courtroom. I was looking at the witness. And I almost feel 04:03:52
like I was about three feet from their face during the time they 04:03:58
testified. So I think that part of it was a non-issue. I think 04:04:03
we're going to see a lot more evidence presented in this format. 04:04:11
Maybe not a full trial, although there's no reason why you 04:04:16
couldn't have a full trial, but I certainly think we're going to 04:04:23
see more evidence presented this way, because I believe having 04:04:26
the witness testify live is more effective than watching a video 04:04:36
of a witness having been examined. And of course having them 04:04:47
testify live means that the Court can ask its own questions, 04:04:53
which is certainly very important with respect to, particularly 04:04:57
with respect to expert witnesses and technical witnesses. So I 04:05:01
expect we'll be seeing a lot more of this. So that will be 04:05:09
interesting. 04:05:22

One of my friends said that -- he's not quite as old 04:05:23
as I am -- but he said that we may have lived in the Golden Age 04:05:27
of civil trial work, because we actually tried some cases over 04:05:36
the years, which is pretty rare nowadays as a percentage, far 04:05:44
more patent cases tried than any other form of civil cases. By 04:05:53
that I mean if you take the total number of patent cases filed 04:06:01
and the number that settled, it wouldn't reach the 98 percent 04:06:05
which applies to civil cases in general. There's going to be 04:06:08

more and more technology involved, I think, particularly in civil cases. I don't know, in criminal cases you've got the confrontation clause, and I'm not sure what exactly will end up satisfying the confrontation clause as far as technology is concerned. That remains to be seen. 04:06:19 04:06:33 04:06:39 04:06:45 04:06:51

But anyway, I think it's worked very well, and I think counsel has been very cooperative and respectful in their presentations through the technology. So that has been a big help. 04:06:54 04:06:58 04:07:09 04:07:14

Is there any -- again, it's somewhat unique the way we're resolving the case, having this extra information supplied on damages. And I think you raised the point, Mr. Jameson, which is certainly a good one, about how we identify exactly what the experts should be doing. And I said that they should analyze the data. I'm not sure exactly how we should define that. I mean, I'm just looking at what the monthly sales are. And I did raise the issue of I don't know what the accounting practices are of Cisco, whether they recognize subscription income on a cash basis or whether they recognize it when the subscription is signed or whether they recognize it one way for tax purposes and another way for other purposes. I don't know. 04:07:24 04:07:34 04:07:45 04:07:55 04:08:03 04:08:16 04:08:23 04:08:33 04:08:36 04:08:45 04:08:58 04:09:01

But when we say we expect the experts to analyze the figure, what do we mean? It seems to me the only thing we mean is that they correctly allocate it to the accused product. I don't think it's any more than that. Does counsel think 04:09:08 04:09:13 04:09:18 04:09:28

otherwise? 04:09:38

MR. JAMESON: No, Your Honor. That's exactly why I 04:09:40 asked the question. I think that if they basically are 04:09:41 explaining, you know, this is the data I received and I did 04:09:47 whatever filtering on it that you need to do to figure out what 04:09:52 are the various monthly revenue numbers, put that into chart 04:09:57 form. And you know, candidly, not that they're going to be, 04:10:03 because the data will be significant, but you know, I would 04:10:09 expect that the numbers that Mr. Gunderson comes up with and Dr. 04:10:14 Becker comes up with, they should look pretty similar to each 04:10:17 other. And then if they don't, obviously it seems to me that 04:10:23 would be a trying to figure out what happened. Where is the 04:10:26 daylight. 04:10:33

THE COURT: Yeah. I think that's right. I would 04:10:34 expect them to be the same. And as far as -- I think I also 04:10:36 mentioned how would that affect your report and/or your opinion, 04:10:43 and they may say not at all. I don't know. I mean, I just 04:10:51 don't know. We don't want them to recalculate damages based on 04:10:58 these figures or come up with a different theory of damages 04:11:06 based on these figures, we just want them to verify that, as 04:11:14 best they can determine, how these figures apply to the accused 04:11:18 products, patent by patent. 04:11:24

Do you have anything further to say about this, Mr. 04:11:39 Andre? 04:11:43

MR. ANDRE: No, Your Honor. When we received the data 04:11:46

originally from Cisco regarding the accused products we got it 04:11:49
on a day-by-day sale, so it was a pretty massive database they 04:11:53
gave us. So we haven't figured out how to calculate that into 04:11:59
month-to-month, because we don't have the program to do it. But 04:12:02
we are still looking into that. But we haven't got the other 04:12:06
legacy products either. So when we get that I think what we 04:12:10
want to do is just give you raw data, you know, put into the 04:12:13
right bucket and not try to do any type of manipulation of that 04:12:17
data, just basically adding it up and putting it in the right 04:12:20
bucket and for the right month. 04:12:23

THE COURT: Well, that's what I had in mind. I don't 04:12:26
know how to define it any further. 04:12:36

MR. JAMESON: And Your Honor, I mean just, I think the 04:12:39
rules of engagement on this project are clear, but we're leaving 04:12:43
this to the experts to do the work, and we're not -- the lawyers 04:12:46
are staying out of it. 04:12:49

THE COURT: Yeah. I mean, I'm not sure if you can 04:12:56
stay completely out of it, because they have got to do it -- 04:13:04
it's got to be based on the accused products and it has to be 04:13:07
based and it has to be done patent-by-patent. 04:13:14

MR. JAMESON: Yeah, I -- 04:13:17

THE COURT: To that extent, I think you have to give 04:13:19
them enough guidance to do that. 04:13:22

MR. JAMESON: Understood, Your Honor. I overstated 04:13:26
"stay out of it", probably. 04:13:28

THE COURT: Okay. All right. Now, any other questions that either side has about what happens now? Have I got your -- 04:13:32 04:13:43 04:13:49

MR. JAMESON: Cisco's were filed. 04:13:56

THE COURT: Have they been delivered? 04:13:59

COURTROOM DEPUTY CLERK: Cisco filed. 04:14:03

LAW CLERK: They have both been filed. 04:14:04

MR. NOONA: They have been filed. 04:14:10

THE COURT: Because I'm not going to be here tomorrow, so I hope we can get them today. Or I hope we have them. 04:14:10 04:14:12

LAW CLERK: We have them. 04:14:21

THE COURT: Do we have them in written form? 04:14:22

LAW CLERK: I don't know if they have been delivered by courier. 04:14:24 04:14:26

THE COURT: Do we have them in written form? 04:14:27

COURTROOM DEPUTY CLERK: They haven't been delivered. They're on ECF right now. They're supposed to deliver them. 04:14:29 04:14:30

MR. JAMESON: Your Honor, I'm told they're enroute from our end. Whatever that means. 04:14:34 04:14:36

COURTROOM DEPUTY CLERK: Okay. 04:14:39

THE COURT: Okay. 04:14:40

MR. ANDRE: I believe Mr. Noona is sending them over from our end as well. 04:14:43 04:14:44

COURTROOM DEPUTY CLERK: Okay. 04:14:46

THE COURT: All right. 04:14:47

MR. ANDRE: I think we're sending two or three copies 04:14:48
over. 04:14:51

COURTROOM DEPUTY CLERK: I'll be here to accept them. 04:14:52
Yes. They were supposed to -- 04:14:55

MR. JAMESON: And Your Honor, we included a signature 04:14:58
block on ours if you just want to sign ours and we could all be 04:15:00
done. 04:15:04

THE COURT: Right. Well, is there anything else 04:15:04
before we adjourn for the day? 04:15:24

MR. ANDRE: Nothing from plaintiff, Your Honor. Thank 04:15:28
you for your time and patience. 04:15:29

MR. JAMESON: And nothing from Cisco, Your Honor. And 04:15:31
I share Mr. Andre's thanks for your perseverance through this. 04:15:33

THE COURT: All right. Well, we'll be adjourned until 04:15:39
whatever date we settled on for the damages argument. 04:15:45

MR. ANDRE: Thank you, Your Honor. 04:15:56

THE COURT: All right. 04:15:56

(Whereupon, proceedings concluded at 4:17 p.m.) 04:15:58

CERTIFICATION

I certify that the foregoing is a true, complete and correct transcript of Volume 22 of the proceedings held in the above-entitled matter.

Paul L. McManus, OCR

Digitally signed by Paul L. McManus, OCR
DN: cn=Paul L. McManus, OCR, c=US, email=pmcmanusocer@verizon.net
Date: 2020.08.10 10:30:29 -04'00'

Paul L. McManus, RMR, FCRR

Date